

Guide de dépannage pour Hybrid Call Service Connect de Cisco Webex

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Informations générales](#)

[Problèmes de configuration des appels](#)

[Échecs du protocole de prise de contact mutuelle TLS](#)

[Conseils utiles de dépannage pour la prise de contact mutuelle TLS](#)

[Problème 1. Expressway-E ne fait pas confiance à l'autorité de certification qui a signé le certificat Cisco Webex](#)

[Problème 2. Nom incorrect pour la vérification du sujet TLS sur Expressway-E Cisco Webex Hybrid DNS Zone](#)

[Problème 3. Expressway-E n'envoie pas la chaîne de certificats complète à Cisco Webex](#)

[Problème 4. Le pare-feu met fin à la prise de contact mutuelle de TLS](#)

[Problème 5. L'Expressway-E est signé par une autorité de certification publique, mais le concentrateur de contrôle Cisco Webex a d'autres certificats chargés](#)

[Problème 6. Expressway ne mappe pas l'appel entrant à la zone DNS hybride Cisco Webex](#)

[Problème 7. Expressway-E utilise un certificat auto-signé par défaut](#)

[Entrant : Cisco Webex vers le site](#)

[Problème 1. Cisco Webex ne peut pas résoudre le SRV/nom d'hôte DNS de l'Expressway-E](#)

[Problème 2. Échec du socket : Port 5062 est bloqué à l'entrée d'Expressway](#)

[Problème 3. Échec du socket : Expressway-E n'est pas à l'écoute sur le port 5062](#)

[Problème 4. Expressway-E ou C ne prend pas en charge les en-têtes de route SIP préchargés](#)

[Problème 5. L'application Cisco Webex reçoit deux notifications d'appel \(toasts\)](#)

[Sortant : Le site vers Cisco Webex](#)

[Problème 1. Expressway ne peut pas résoudre l'adresse callservice.ciscopark.com](#)

[Problème 2. Le port 5062 est bloqué en sortie vers Cisco Webex](#)

[Problème 3. Erreur de configuration de la règle de recherche Expressway](#)

[Problème 4. Erreur de configuration CPL Expressway](#)

[Bidirectionnel : Cisco Webex vers le site ou le site vers Cisco Webex](#)

[Problème 1. Le téléphone IP/terminal de collaboration offre un codec audio autre que G.711, G.722 ou AAC-LD.](#)

[Problème 2. Taille maximale du message entrant Unified CM dépassée](#)

[Annexe](#)

[Outils de dépannage Expressway](#)

[Fonction de vérification de schéma](#)

[Fonction de localisation](#)

[Journaux de diagnostic](#)

[Informations connexes](#)

Introduction

Ce document décrit la solution Cisco Webex Hybride Call Service Connect, qui permet à votre infrastructure actuelle de contrôle des appels de Cisco de se connecter au nuage Cisco Collaboration Cloud de façon à ce qu'ils puissent fonctionner ensemble.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissance de l'offre Cisco Webex
- Connaissance de la solution Expressway (B2B)
- Connaissance de Cisco Unified Communications Manager (Unified CM) et de son intégration dans Expressway
- Unified CM 10.5 (2) SU5 ou versions ultérieures.
- Expressway (B2B) version X8.7.1 ou ultérieure (la version X8.9.1 est recommandée)
- Expressway (Connector Host) — Voir [Prise en charge des hôtes de connecteur Expressway pour les services hybrides Cisco Webex](#) pour les versions actuellement prises en charge

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Solutions Cisco Unified Communications Manager
- Expressways
- Webex pour Windows
- Webexfor Mac
- Webexfor iOS
- Webex pour Android
- Terminaux de collaboration de Cisco
- Terminaux de collaboration de bureau
- Téléphones IP
- Clients logiciels

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

La solution offre les fonctionnalités suivantes :

- Utiliser l'application Webex comme client logiciel mobile pour les appels audio et vidéo
- Utiliser l'application pour passer et recevoir des appels n'importe où, comme au bureau

- Utiliser Webex, Cisco Jabber ou leur téléphone de bureau pour appeler, sans avoir à se soucier de l'option qu'ils utilisent
- Déverrouiller l'historique des appels sur les téléphones sur site et intégrer cet historique dans Webex

Ce guide porte sur les problèmes qui sont uniques à la solution Hybride Call Service Connect. Étant donné que Hybrid Call Service Connect fonctionne sur la même paire Expressway E & C que d'autres solutions telles que Mobile and Remote Access et Business to Business, les problèmes avec les autres solutions peuvent affecter Hybrid Call Service Connect. Pour les clients et partenaires qui déploient une paire Expressway pour une utilisation avec Call Service Connect, le [guide de configuration de base de Cisco VCS Expressway et VCS Control doit être consulté avant toute tentative de déploiement de Hybrid Call Service Connect](#). Ce guide de dépannage couvre les considérations relatives au pare-feu/NAT ainsi que la conception d'Expressway dans les annexes 3 et 4. Examinez attentivement cette documentation. En outre, ce document se fonde sur la supposition que l'activation de l'hôte connecteur Expressway et des services hybrides Hybrid Call Service a été effectuée.

Problèmes de configuration des appels

Échecs du protocole de prise de contact mutuelle TLS

Hybrid Call Service Connect fait appel à des mesures de sécurité de couches de transport (TLS mutuelle) pour les démarches d'authentification entre Cisco Webex et Expressway-E. Cela signifie qu'Expressway-E et Cisco Webex vérifient et examinent le certificat présenté par l'autre. Étant donné que les problèmes de TLS mutuels sont très répandus lors des nouveaux déploiements des serveurs Expressway et de l'activation de solutions telles que Hybrid Call Service Connect, cette section fournit des informations et des conseils utiles pour le dépannage des problèmes basés sur des certificats entre les Expressways et Cisco Webex.

Que vérifie Expressway-E?

- Est-ce que le certificat Cisco Webex a été signé par une CA publique qui est répertoriée dans la liste de CA de confiance d'Expressway-E?
- Est-ce que `callservice.ciscopark.com` apparaît dans le champ de l'autre nom du sujet du certificat Cisco Webex?

Que vérifie Cisco Webex?

- Est-ce que le certificat d'Expressway-E a été signé par l'une des CA publiques réputées fiables par Webex? ([Liste des CA de confiance de Cisco Webex](#))
- Si l'Expressway-E n'utilise pas un certificat signé de façon publique, est-ce que le certificat d'Expressway et les éventuels certificats racines et intermédiaires ont été téléchargés vers le concentrateur Cisco Webex Control Hub (<https://admin.ciscopark.com>)?

Cela s'explique comme l'illustre l'image.



Conseils utiles de dépannage pour la prise de contact mutuelle TLS

1. Décoder la prise de contact mutuelle TLS

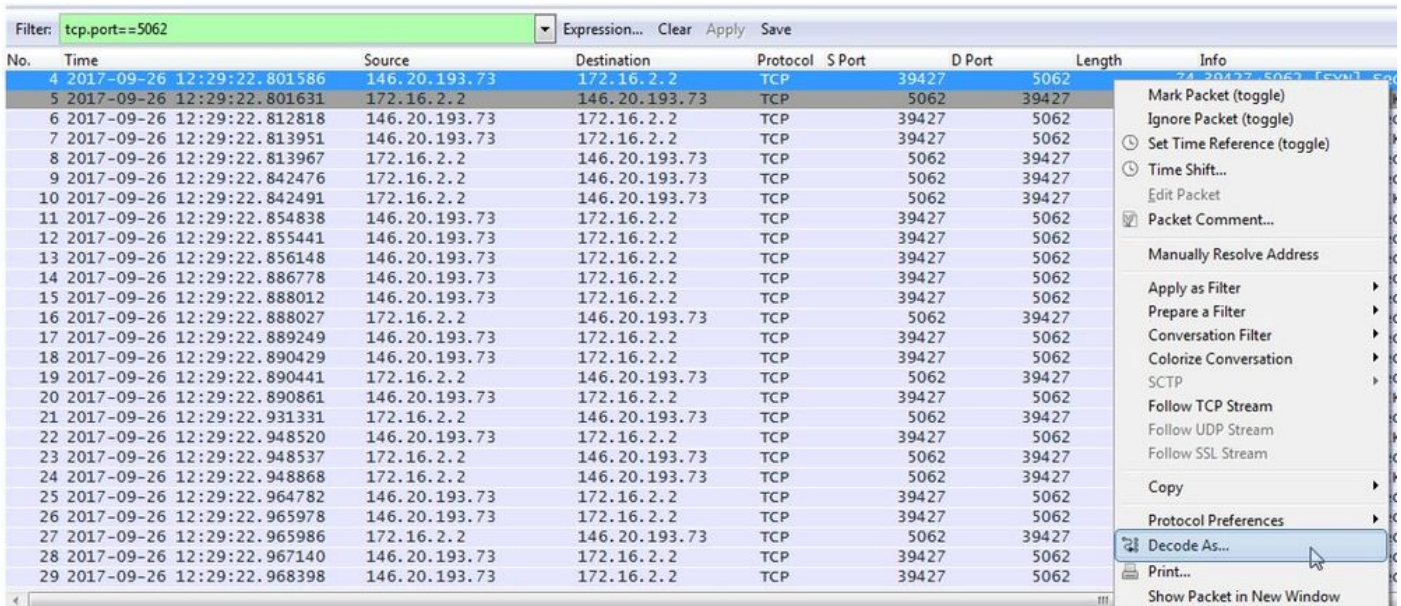
Par défaut, Wireshark marque le trafic TLS de SIP comme le port 5061. Cela signifie que chaque fois que vous voulez analyser une connexion TLS (mutuelle) qui se produit sur le port 5062, Wireshark ne saura pas comment décoder correctement le trafic. Voici un exemple de processus de prise de contact mutuelle sur le port 5062, comme l'illustre l'image.

No.	Time	Source	Destination	Protocol	S Port	D Port	Length	Info
169	2017-09-20 14:22:13.293817	146.20.193.45	172.16.2.2	TCP	48520	5062	74	48520->5062 [SYN] Seq=0 Win=14600 Len=0 MSS=1380 SACK_PERM=1 TSval=3875387337 TSecr=0 WS=128
170	2017-09-20 14:22:13.293846	172.16.2.2	146.20.193.45	TCP	5062	48520	74	5062->48520 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=444315393 TSecr=
171	2017-09-20 14:22:13.304549	146.20.193.45	172.16.2.2	TCP	48520	5062	66	48520->5062 [ACK] Seq=1 Ack=1 Win=14720 Len=0 TSval=3875387348 TSecr=444315393
172	2017-09-20 14:22:13.305898	146.20.193.45	172.16.2.2	TCP	48520	5062	266	48520->5062 [PSH, ACK] Seq=1 Ack=1 Win=14720 Len=200 TSval=3875387349 TSecr=444315393
173	2017-09-20 14:22:13.305911	172.16.2.2	146.20.193.45	TCP	5062	48520	66	5062->48520 [ACK] Seq=1 Ack=201 Win=30080 Len=0 TSval=444315405 TSecr=3875387349
174	2017-09-20 14:22:13.336342	172.16.2.2	146.20.193.45	TCP	5062	48520	2802	5062->48520 [ACK] Seq=1 Ack=201 Win=30080 Len=2736 TSval=444315436 TSecr=3875387349
175	2017-09-20 14:22:13.336358	172.16.2.2	146.20.193.45	TCP	5062	48520	1426	5062->48520 [PSH, ACK] Seq=2737 Ack=201 Win=30080 Len=1360 TSval=444315436 TSecr=3875387349

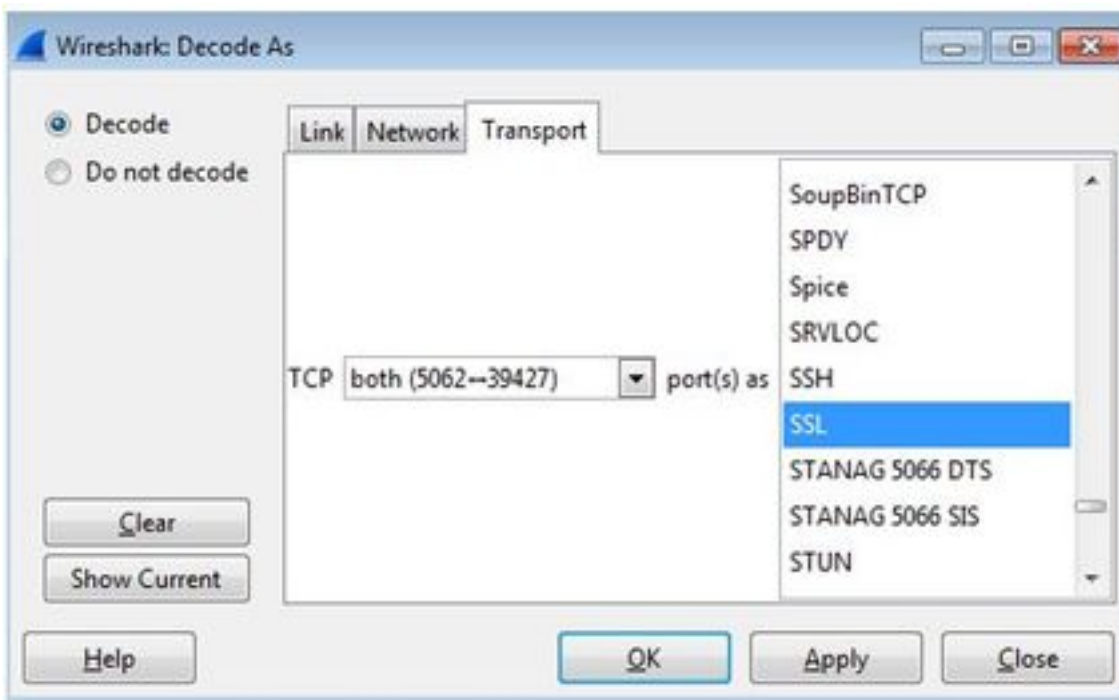
Vous pourrez observer de quelle façon une prise de contact mutuelle se présente dans Wireshark. Le paquet numéro 175 est le certificat qu'Expressway envoie à Cisco Webex. Cependant, vous ne pouvez pas le déterminer sans que le trafic soit décodé. Il y a deux méthodes possibles pour décoder ce trafic afin que vous puissiez plus facilement visualiser l'information des certificats et les messages d'erreur susceptibles de se présenter.

1 bis. Décoder le flux en tant que SSL

a. Lorsque vous analysez la prise de contact mutuelle de TLS, dans un premier temps, filtrez la capture par `tcp.port==5062`. Après cela, cliquez avec le bouton droit sur le premier paquet du flux et sélectionnez **Décoder sous...** comme le montre l'image.



b. Une fois le **Decode As...** est sélectionnée, vous voyez une liste dans laquelle vous pouvez sélectionner comment décoder le flux que vous avez sélectionné. Dans la liste, sélectionnez **SSL**, cliquez sur **Apply** et fermez la fenêtre. À ce stade, l'ensemble du flux montre le certificat et les messages d'erreur échangés au moment de la prise de contact, comme l'illustre l'image.



1 ter. Modifier le port TLS de SIP

Lorsque vous modifiez le port SIP de TLS pour qu'il porte le numéro 5062 dans les préférences de Wireshark, vous pouvez ensuite consulter tous les détails de la prise de contact, y compris les certificats. Afin de faire cette modification :

- Ouvrez Wireshark
- Naviguez jusqu'à **Edit > Preferences**
- Dans les protocoles, choisissez **SIP**
- Définissez le port TLS de SIP comme 5062, puis cliquez sur Appliquer
- Remplacez la valeur par 5061 lorsque l'analyse est terminée, comme le montre l'image.

SIP TCP ports:

SIP TLS Port:

Display raw text for SIP message:

Si vous analysez maintenant la même capture, vous verrez que les paquets 169 à 175 sont décodés. Le paquet 175 montre le certificat d'Expressway-E. Si vous analysez le paquet, vous pouvez voir tous les détails de certificat, comme l'indique l'image.

No.	Time	Source	Destination	Protocol	S Port	D Port	Length	Info
169	2017-09-20 14:22:13.293817	146.20.193.45	172.16.2.2	TCP	48520	5062	74	48520->5062 [SYN] Seq=0 Win=14600 Len=0 MSS=1380 SACK_PERM=1 TSval=3875387337 TSecr=0 WS=128
170	2017-09-20 14:22:13.293846	172.16.2.2	146.20.193.45	TCP	5062	48520	74	5062->48520 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=444315393 TSecr=3875387337 WS=128
171	2017-09-20 14:22:13.304549	146.20.193.45	172.16.2.2	TCP	48520	5062	66	48520->5062 [ACK] Seq=1 Ack=1 Win=14720 Len=0 TSval=3875387348 TSecr=444315393
172	2017-09-20 14:22:13.305898	146.20.193.45	172.16.2.2	TLSv1.1	48520	5062	266	Client Hello
173	2017-09-20 14:22:13.305911	172.16.2.2	146.20.193.45	TCP	5062	48520	66	5062->48520 [ACK] Seq=1 Ack=201 Win=30080 Len=0 TSval=444315405 TSecr=3875387349
174	2017-09-20 14:22:13.336342	172.16.2.2	146.20.193.45	TLSv1.1	5062	48520	2802	Server Hello
175	2017-09-20 14:22:13.336358	172.16.2.2	146.20.193.45	TLSv1.1	5062	48520	1426	Certificate

2. Filtre Wireshark

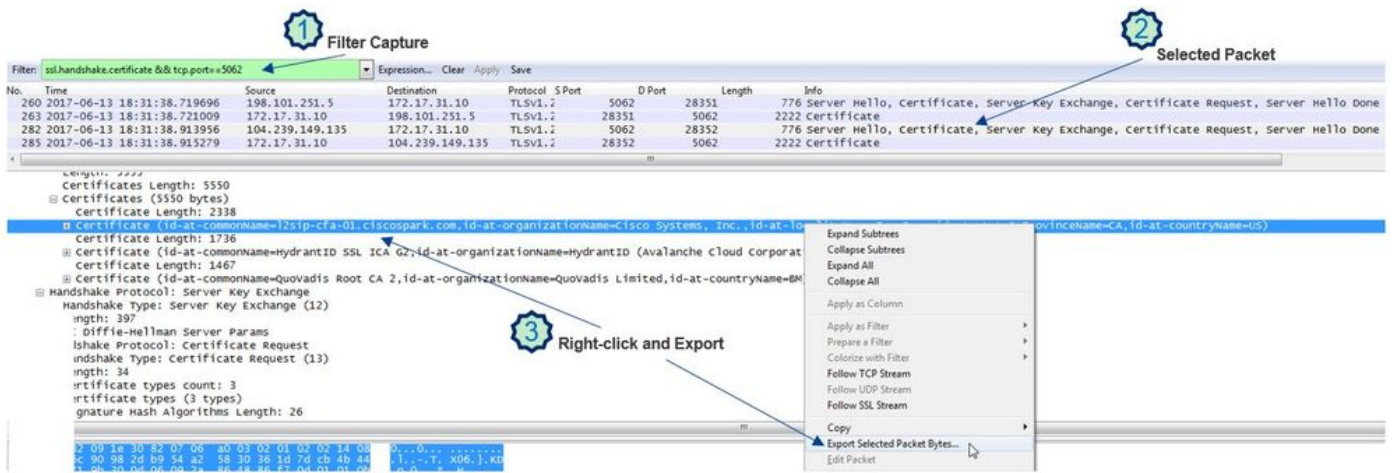
Lorsque vous analysez les captures de paquets, il est facile de se perdre parmi les nombreux paquets observés dans une capture donnée. Il est important de comprendre quel type de trafic vous intéresse le plus, afin que vous puissiez appliquer un filtre Wireshark pour qu'il affiche seulement ce que vous souhaitez consulter. Voici certains des filtres Wireshark courants qui peuvent vous permettre d'obtenir de plus amples renseignements sur une prise de contact mutuelle de TLS :

- `tcp.port==5062`
- `ssl && tcp.port==5062`
- `ssl.handshake.certificate && tcp.port==5062`

3. Extrayez le certificat de Pcap

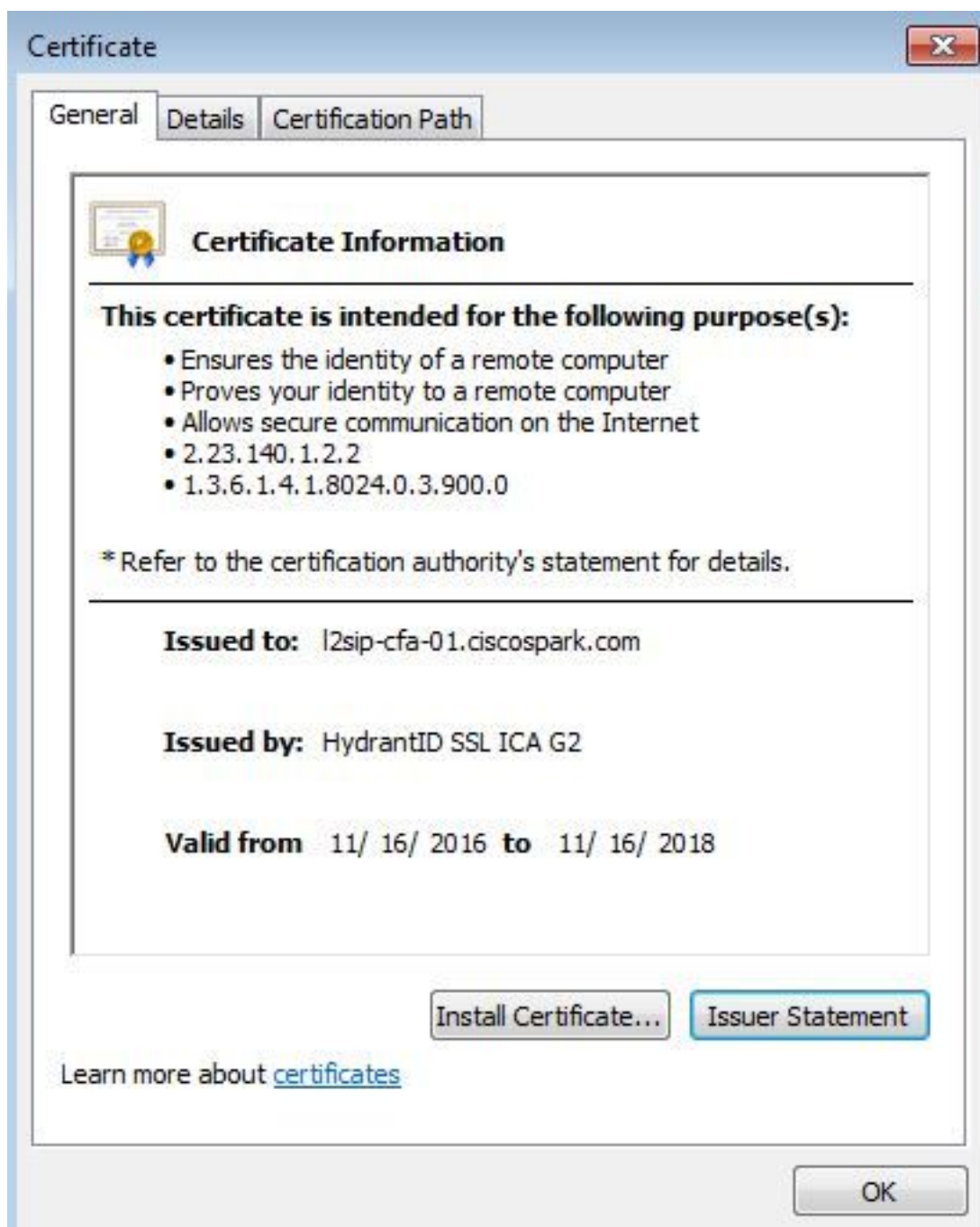
De temps à autre, vous devrez peut-être obtenir une copie d'un certificat (serveur, racine ou intermédiaire). Si vous ne connaissez pas où trouver le certificat que vous êtes dans recherchez, vous pouvez le extraire directement à partir de une saisie de paquets. Voici les étapes à suivre pour obtenir le certificat de Cisco Webex qui est présenté lors d'une prise de contact mutuelle de TLS.

1. Filtrer la capture de paquets avec `ssl.handshake.certificate && tcp.port==5062`
2. Repérez le paquet qui provient de l'adresse de serveur de Webex. Le certificat apparaît dans la section de l'information.
3. Dans les détails du paquet, développez **Secure Socket Layer > TLS Certificate > Handshake Protocol > Certificates**. **Note:** Le dernier certificat (en bas) de la chaîne de certificats provient de l'autorité de certification racine.
4. Cliquez avec le bouton droit sur le certificat d'intérêt et sélectionnez **Exporter les octets de paquets sélectionnés...** comme le montre l'image.



5. Enregistrez le fichier sous le format .cer.

6. Cliquez deux fois sur le fichier enregistré pour ouvrir le certificat, comme l'indique l'image.



4. Réglez les niveaux de journalisation d'Expressway

Deux modules de journalisation sont disponibles sur Expressway. Ils peuvent vous aider à mieux comprendre la logique qu'applique Expressway lorsque vous analysez les certificats :

- developer.ssl
- developer.zone.zonemg

Par défaut, ces modules de journalisation sont réglés à un niveau d'information (INFO). Lorsque les modules sont définis selon un niveau de débogage (DEBUG), vous pouvez consulter les renseignements concernant l'inspection de certificat qui se déroule, de même que de l'information sur le trafic de zone cartographié. Ces deux fonctions sont pertinentes pour Hybrid Call Service.

Un exemple de l'Expressway-E qui effectue une inspection SAN du certificat de serveur de Cisco Webex.

```
2017-09-22T11:11:19.485-04:00 amer-expressway01 tvcs: UTCTime="2017-09-22 15:11:19,485"
Module="developer.ssl" Level="INFO" CodeLocation="ppcmains/ssl/ttssl/ttssl_openssl.cpp(1974) "
Method="::ttssl_continueHandshake" Thread="0x7f576cbee700": Detail="Handshake in progress"
Reason="want read/write"
2017-09-22T11:11:19.564-04:00 amer-expressway01 tvcs: UTCTime="2017-09-22 15:11:19,564"
Module="developer.ssl" Level="DEBUG" CodeLocation="ppcmains/ssl/ttssl/ttssl_openssl.cpp(1960) "
Method="::ttssl_continueHandshake" Thread="0x7f576cbee700": Detail="Handshake succeeded"
2017-09-22T11:11:19.564-04:00 amer-expressway01 tvcs: UTCTime="2017-09-22 15:11:19,564"
Module="developer.ssl" Level="DEBUG" CodeLocation="ppcmains/ssl/ttssl/ttssl_openssl.cpp(1629) "
Method="::TTSSL_retrieveCommonName" Thread="0x7f576cbee700": Detail="Found common name in peer
certificate" CommonName="l2sip-cfa-01.ciscospark.com"
2017-09-22T11:11:19.564-04:00 amer-expressway01 tvcs: UTCTime="2017-09-22 15:11:19,564"
Module="developer.ssl" Level="DEBUG" CodeLocation="ppcmains/ssl/ttssl/ttssl_openssl.cpp(1654) "
Method="::TTSSL_retrieveAltNames" Thread="0x7f576cbee700": Detail="Found DNS alt-name in peer
certificate" AltName="l2sip-cfa-01.ciscospark.com"
2017-09-22T11:11:19.564-04:00 amer-expressway01 tvcs: UTCTime="2017-09-22 15:11:19,564"
Module="developer.ssl" Level="DEBUG" CodeLocation="ppcmains/ssl/ttssl/ttssl_openssl.cpp(1654) "
Method="::TTSSL_retrieveAltNames" Thread="0x7f576cbee700": Detail="Found DNS alt-name in peer
certificate" AltName="l2sip-cfa-01.wbx2.com"
2017-09-22T11:11:19.564-04:00 amer-expressway01 tvcs: UTCTime="2017-09-22 15:11:19,564"
Module="developer.ssl" Level="DEBUG" CodeLocation="ppcmains/ssl/ttssl/ttssl_openssl.cpp(1654) "
Method="::TTSSL_retrieveAltNames" Thread="0x7f576cbee700": Detail="Found DNS alt-name in peer
certificate" AltName="l2sip-cfa-01-web.wbx2.com"
2017-09-22T11:11:19.564-04:00 amer-expressway01 tvcs: UTCTime="2017-09-22 15:11:19,564"
Module="developer.ssl" Level="DEBUG" CodeLocation="ppcmains/ssl/ttssl/ttssl_openssl.cpp(1654) "
Method="::TTSSL_retrieveAltNames" Thread="0x7f576cbee700": Detail="Found DNS alt-name in peer
certificate" AltName="l2sip-cfa-web.wbx2.com"
2017-09-22T11:11:19.564-04:00 amer-expressway01 tvcs: UTCTime="2017-09-22 15:11:19,564"
Module="developer.ssl" Level="DEBUG" CodeLocation="ppcmains/ssl/ttssl/ttssl_openssl.cpp(1654) "
Method="::TTSSL_retrieveAltNames" Thread="0x7f576cbee700": Detail="Found DNS alt-name in peer
certificate" AltName="callservice.ciscospark.com"
2017-09-22T11:11:19.564-04:00 amer-expressway01 tvcs: UTCTime="2017-09-22 15:11:19,564"
Module="developer.ssl" Level="DEBUG" CodeLocation="ppcmains/ssl/ttssl/ttssl_openssl.cpp(1654) "
Method="::TTSSL_retrieveAltNames" Thread="0x7f576cbee700": Detail="Found DNS alt-name in peer
certificate" AltName="callservice.call.ciscospark.com"
```

Exemple d'Expressway-E mappant la connexion MTLs à la zone DNS hybride Cisco Webex :

```
2017-09-22T11:11:19.564-04:00 amer-expressway01 tvcs: UTCTime="2017-09-22 15:11:19,564"
Module="developer.zone.zonemgr" Level="DEBUG"
CodeLocation="ppcmains/oak/zones/ZoneManager.cpp(1226) "
```



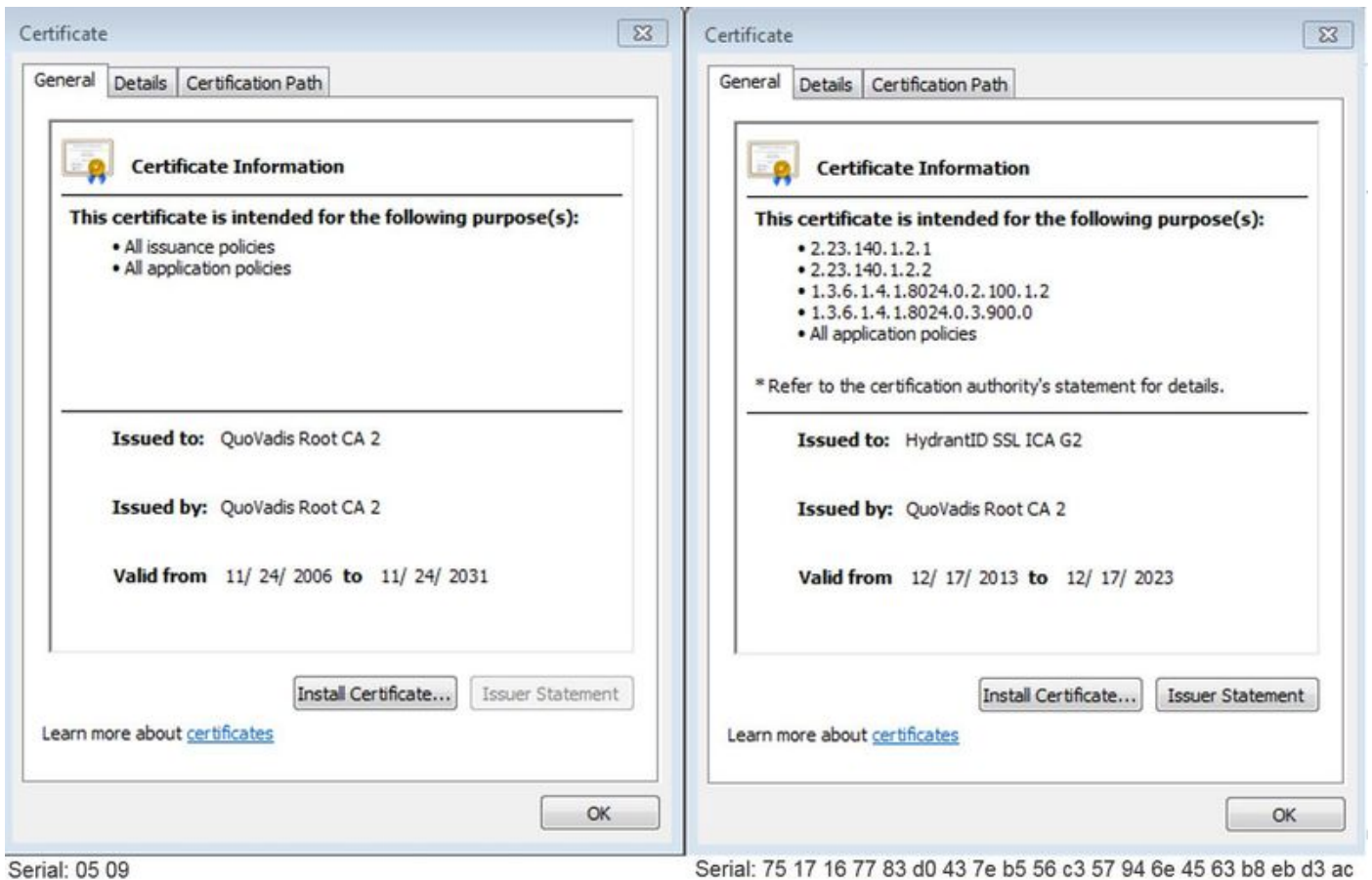
```
Method="ZoneManager::getDNSZoneByTLSVerifySubjectName" Thread="0x7f577f0a0700":
this="0x56408ff81220" getDNSZoneByTLSVerifySubjectName classified subject name
callservice.ciscospark.com into DNS zone Hybrid Call Services DNS
2017-09-22T11:11:19.564-04:00 amer-expressway01 tvcs: UTCTime="2017-09-22 15:11:19,564"
Module="developer.zone.zonemgr" Level="DEBUG"
CodeLocation="ppcmains/oak/zones/ZoneManager.cpp(1183) "
Method="ZoneManager::getDNSZoneByTLSVerifySubjectNameList" Thread="0x7f577f0a0700":
this="0x56408ff81220" Detail="Searched for DNS Zones by Subject Name" Found="True"
Candidates="l2sip-cfa-01.ciscospark.coml2sip-cfa-01.ciscospark.coml2sip-cfa-01.wbx2.coml2sip-
cfa-01-web.wbx2.coml2sip-cfa-web.wbx2.comcallservice.ciscospark.com" MatchedZone="Hybrid Call
Services DNS" MatchedIdentity="callservice.ciscospark.com"
2017-09-22T11:11:19.564-04:00 amer-expressway01 tvcs: UTCTime="2017-09-22 15:11:19,564"
Module="developer.zone.zonemgr" Level="DEBUG"
CodeLocation="ppcmains/oak/zones/ZoneManager.cpp(1054) "
Method="ZoneManager::getZoneByIdentities" Thread="0x7f577f0a0700": this="0x56408ff81220"
Detail="getZoneByIdentities, match complete" Identitites="{CN: l2sip-cfa-01.ciscospark.com, Alt-
DNS: l2sip-cfa-01.ciscospark.com, Alt-DNS: l2sip-cfa-01.wbx2.com, Alt-DNS: l2sip-cfa-01-
web.wbx2.com, Alt-DNS: l2sip-cfa-web.wbx2.com, Alt-DNS: callservice.ciscospark.com, Alt-DNS:
callservice.call.ciscospark.com, Alt-DNS: l2sip-a-Webexcall.ciscospark.com, Alt-DNS: l2sip-prod-
11-dfw-public.wbx2.com, Alt-DNS: l2sip-prod-12-dfw-public.wbx2.com, Alt-DNS: l2sip-l2sipproda1-
294-riiad-public.wbx2.com, Alt-DNS: l2sip-l2sipproda1-817-riiad-public.wbx2.com, Alt-DNS: l2sip-
l2sip-prod-wpsjc-web.ciscospark.com, Alt-DNS: l2sip-l2sip-prod-wpsjc-web.wbx2.com, Alt-DNS:
l2sip-l2sip-prod-wpdfw-web.ciscospark.com, Alt-DNS: l2sip-l2sip-prod-wpdfw-web.wbx2.com, Alt-
DNS: l2sip-cfa-02.wbx2.com, Alt-DNS: Webexcmr-wpa.ciscospark.com, Alt-DNS: Webexcmr-
wpb.ciscospark.com, Alt-DNS: Webexcmr-wpc.ciscospark.com, Alt-DNS: l2sip-wpa-01.wbx2.com, Alt-
DNS: l2sip-wpa-02.wbx2.com, Alt-DNS: l2sip-wpb-01.wbx2.com, Alt-DNS: l2sip-wpb-02.wbx2.com, Alt-
DNS: l2sip-wpc-01.wbx2.com, Alt-DNS: l2sip-wpc-02.wbx2.com}" MatchMechanism="DNSZoneMatch"
MatchedZone="Hybrid Call Services DNS"
```

Voici une liste des problèmes les plus courants liés aux défaillances de TLS lors des processus mutuels entre l'Expressway-E et Cisco Webex.

Problème 1. Expressway-E ne fait pas confiance à l'autorité de certification qui a signé le certificat Cisco Webex

Le serveur de Cisco Webex qui est en communication directe avec l'Expressway-E est appelé serveur L2SIP. Ce serveur L2SIP doit faire l'objet d'une signature d'autorisation par un serveur intermédiaire portant le nom courant de **Hydrant SSL ICA G2**. Le serveur intermédiaire doit faire l'objet d'une signature d'autorisation par une autorité de certification racine portant le nom courant de **QuoVadis Root CA 2**, comme l'indique l'image.

Note: Cela pourrait faire l'objet de modifications.



Serial: 05 09

Serial: 75 17 16 77 83 d0 43 7e b5 56 c3 57 94 6e 45 63 b8 eb d3 ac

La première étape pour analyser ce trafic sous l'angle d'un diagnostic Expressway consiste à faire des recherches portant sur les connexions TCP : **TCP Connecting**. Une fois que vous aurez repéré **TCP Connecting**, cherchez la valeur **Dst-port=5062**. Une fois que vous aurez cerné dans les journaux la zone où cette connexion a été tentée et établie, vous pourrez chercher à repérer la prise de contact mutuelle de TLS, qui apparaît généralement dans les entrées de journal qui indiquent que le processus est en cours (Handshake in progress).

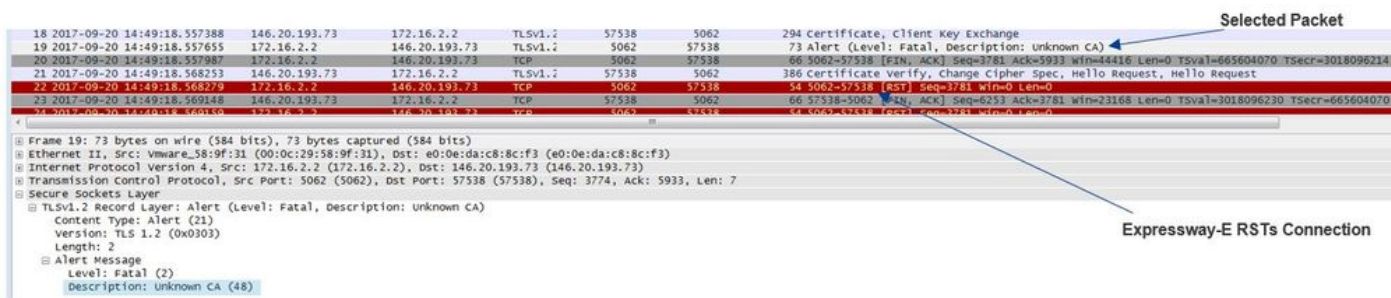
```
2017-09-20T10:49:18.427-04:00 amer-expressway01 tvcs: UTCTime="2017-09-20 14:49:18,426"
Module="developer.ssl" Level="INFO" CodeLocation="ppcmains/ssl/ttssl/ttssl_openssl.cpp(1974) "
Method="::ttssl_continueHandshake" Thread="0x7f29ddefa700": Detail="Handshake in progress"
Reason="want read/write"
```

Si l'Expressway-E ne tient pas les certificats de Cisco Webex signés pour des certificats fiables, il est fort probable que l'Expressway-E rejette le certificat tout de suite après l'achèvement du processus de prise de contact. Vous pourrez trouver des traces de ces actions dans les journaux d'Expressway-E, en particulier dans ces entrées de journal :

```
2017-09-20T10:49:18.724-04:00 amer-expressway01 tvcs: Event="Inbound TLS Negotiation Error"
Service="SIP" Src-ip="146.20.193.73" Src-port="58531" Dst-ip="172.16.2.2" Dst-port="5062"
Detail="self signed certificate in certificate chain" Protocol="TLS" Level="1" UTCTime="2017-09-20
20 14:49:18,724"
2017-09-20T10:49:18.724-04:00 amer-expressway01 tvcs: UTCTime="2017-09-20 14:49:18,724"
Module="developer.ssl" Level="ERROR" CodeLocation="ppcmains/ssl/ttssl/ttssl_openssl.cpp(68) "
Method="::TTSSL_ErrorOutput" Thread="0x7f29ddefa700": TTSSL_continueHandshake: Failed to
establish SSL connection iResult="-1" error="1" bServer="true"
localAddress="['IPv4','TCP','172.16.2.2:5062']" remoteAddress="['IPv4','TCP','146.20.193.73:58531']"
ssl_error_reason="error:14089086:SSL routines:ssl3_get_client_certificate:certificate verify
failed"
2017-09-20T10:49:18.724-04:00 amer-expressway01 tvcs: UTCTime="2017-09-20 14:49:18,724"
Module="network.tcp" Level="DEBUG": Src-ip="146.20.193.73" Src-port="58531" Dst-ip="172.16.2.2"
Dst-port="5062" Detail="TCP Connection Closed" Reason="self signed certificate in certificate
```

chain"

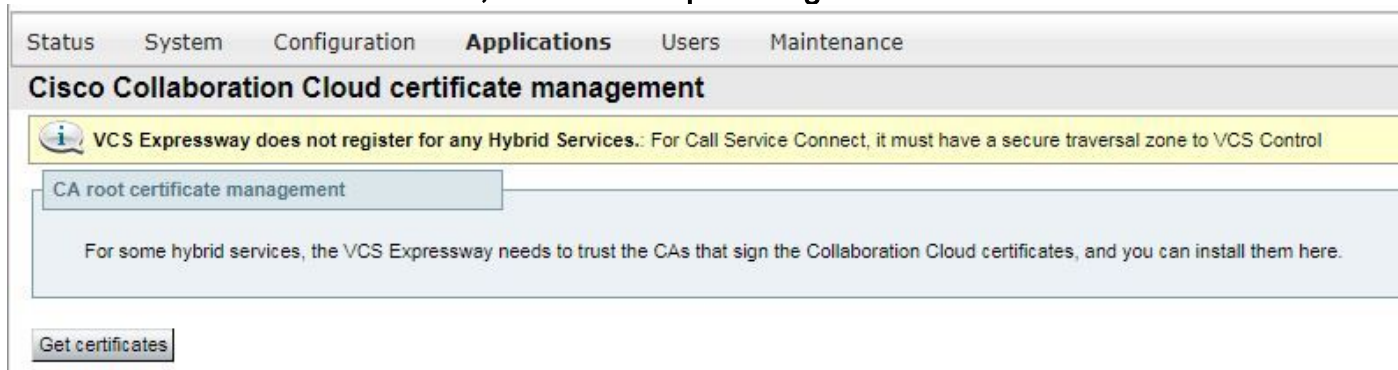
Le message d'erreur d'Expressway peut induire légèrement en erreur car il fait référence à un certificat auto-signé dans la chaîne de certificats. Wireshark vous permet de regarder de plus près l'échange. Du point de vue de l'analyse de capture de paquets Wireshark, vous pouvez clairement voir que lorsque l'environnement Webex présente son certificat, Expressway se retourne et rejette avec un certificat avec une erreur de CA inconnue, comme le montre l'image.



Solution :

Afin de résoudre cette situation, vous devez vérifier que l'Expressway-E tient pour fiables les autorités de certification de Cisco Webex. Tandis que vous pourriez simplement extraire ces certificats d'une trace Wireshark et les télécharger dans le centre de certificats des autorités de certification de confiance (Trusted CA) de l'Expressway, l'Expressway offre une méthode plus simple :

- Ouvrez une session dans l'Expressway-E
- Accédez à **Applications > Gestion des certificats cloud**
- Sélectionnez **Get Certificates**, comme l'indique l'image.



À ce stade-là, les autorités de certification de Cisco Webex sont téléversés dans le centre Trusted CA d'Expressway-E (**Maintenance > Security > Trusted CA certificate**).

Problème 2. Nom incorrect pour la vérification du sujet TLS sur Expressway-E Cisco Webex Hybrid DNS Zone

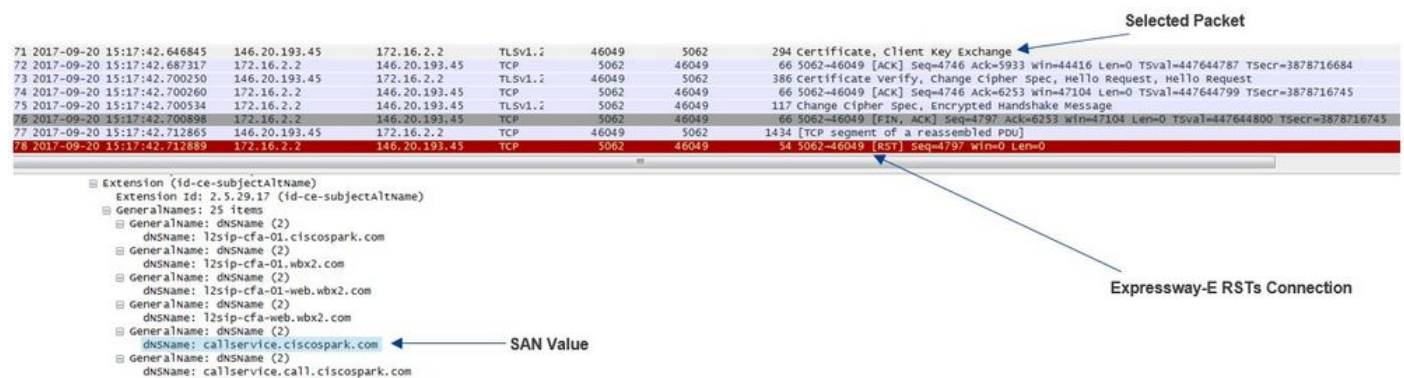
Dans le cadre de la prise de contact mutuelle de TLS, Hybrid Call Service Connect fait appel à la vérification de TLS. Cela signifie qu'en plus de se fier aux certificats de CA de Cisco Webex, l'Expressway vérifie le certificat en contrôlant le champ SAN (Subject Alternate Name, autres noms de sujet) du certificat présenté pour vérifier qu'il a une valeur, comme celle de **callservice.ciscospark.com** . Si cette valeur n'est pas présente, il y aura un échec de l'appel entrant.

Dans ce scénario particulier, le serveur Cisco Webex présente son certificat à l'Expressway-E. Dans les faits, le certificat a 25 noms de sujets (SAN) différents. Envisagez un cas où

l'Expressway-E vérifierait le certificat pour le SAN `callservice.ciscopark.com` sans trouver ce nom de sujet. Dans un tel cas, vous pourrez voir une erreur semblable à celle-ci dans les journaux de diagnostic :

```
2017-09-20T11:17:42.701-04:00 amer-expressway01 tvcs: Event="Inbound TLS Negotiation Error"
Service="SIP" Src-ip="146.20.193.45" Src-port="46049" Dst-ip="172.16.2.2" Dst-port="5062"
Detail="Peer's TLS certificate identity was unacceptable" Protocol="TLS" Level="1"
UTCTime="2017-09-20 15:17:42,700"
2017-09-20T11:17:42.701-04:00 amer-expressway01 tvcs: UTCTime="2017-09-20 15:17:42,700"
Module="network.tcp" Level="DEBUG": Src-ip="146.20.193.45" Src-port="46049" Dst-ip="172.16.2.2"
Dst-port="5062" Detail="TCP Connection Closed" Reason="Peer's TLS certificate identity was
unacceptable"
```

Si vous utilisez Wireshark pour analyser la prise de contact pour ce certificat, vous pourrez constater qu'après la présentation par Cisco Webex d'un certificat, l'Expressway ne tarde pas à mettre fin à la connexion (arrêt RST), comme l'indique l'image.



Afin de confirmer la configuration de cette valeur, vous pouvez accéder à la zone DNS de Webex Hybrid qui a été configurée pour la solution. Si vous avez la xConfiguration Expressway-E, vous pouvez consulter la section de configuration de la zone pour déterminer comment le nom de sujet de vérification de TLS a été configuré. Pour xConfiguration, notez que les zones sont présentées en ordre, la Zone 1 en premier. Voici une xConfiguration provenant de l'environnement problématique analysé ci-dessus.

```
*c xConfiguration Zones Zone 6 DNS SIP TLS Verify Mode: "On"
*c xConfiguration Zones Zone 6 DNS SIP TLS Verify Subject Name: "call1service.ciscopark.com"
```

Comme vous pouvez le voir dans l'exemple, le nom du sujet de vérification TLS est défini sur `call1service.ciscopark.com` au lieu de `callservice.ciscopark.com`. (notez le « 1 » supplémentaire).

Solution :

Afin de résoudre ce problème, le nom de sujet de vérification de TLS doit être modifié comme suit :

- Ouvrez une session dans l'Expressway-E
- Naviguez jusqu'à **Configuration > Zones > Zones**
- Sélectionnez **Webex Hybrid Services DNS Zone**
- Définissez le nom de sujet de vérification (TLS verify subject name) comme suit : `callservice.ciscopark.com`
- Sélectionnez **Save (enregistrer)**

Note: Par la suite, consultez le comportement de journalisation de référence. Cette section

présente la vérification du certificat s'exécutant sur Expressway, de même que la mise en correspondance des données de la zone DNS de Webex Hybrid.

Note: Depuis le code Expressway x12.5 et les versions ultérieures, une nouvelle zone « Webex » est sortie. Cette zone Webex préremplit la configuration de la zone requise pour la communication vers Webex. Cela signifie que vous n'avez plus besoin de définir le mode de vérification de l'objet TLS et le nom de l'objet de vérification TLS. Pour simplifier la configuration, il est recommandé d'utiliser la zone Webex si vous utilisez x12.5 ou une version ultérieure du code Expressway.

Problème 3. Expressway-E n'envoie pas la chaîne de certificats complète à Cisco Webex

Dans le cadre de la prise de contact mutuelle de TLS, Cisco Webex doit se fier au certificat d'Expressway-E. Cisco Webex a une liste complète de ses CA publiques de confiance. En général, une prise de contact mutuelle de TLS est menée à bien lorsque votre certificat d'Expressway-E est signé par une autorité de certification publique que prend en charge Cisco Webex. Par conception, l'Expressway-E n'envoie son certificat qu'au cours d'une connexion TLS, bien qu'il ait été signé par une autorité de certification publique. Afin d'envoyer la chaîne complète de certificats (racine et intermédiaire), ces certificats doivent être ajoutés au magasin de certificats CA de confiance sur l'Expressway-E lui-même.

Si cette condition n'est respectée, Cisco Webex rejette le certificat d'Expressway-E. Lorsque vous faites du dépannage dans une situation qui correspond à ce problème, vous pouvez utiliser les journaux de diagnostic et tcpdump dans l'Expressway-E. Lorsque vous analysez les journaux de diagnostic d'Expressway-E, vous observerez une erreur semblable à celle-ci :

```
2017-09-19T11:12:09.721-04:00 amer-expressway01 tvcs: Event="Inbound TLS Negotiation Error"
Service="SIP" Src-ip="146.20.193.45" Src-port="33441" Dst-ip="172.16.2.2" Dst-port="5062"
Detail="sslv3 alert certificate unknown" Protocol="TLS" Level="1" UTCTime="2017-09-19
15:12:09,721"
2017-09-19T11:12:09.721-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 15:12:09,721"
Module="developer.ssl" Level="ERROR" CodeLocation="ppcmains/ssl/ttssl/ttssl_openssl.cpp(68)"
Method=":TTSSLErrorOutput" Thread="0x7fc67c6ec700": TTSSL_continueHandshake: Failed to
establish SSL connection iResult="0" error="1" bServer="true"
localAddress="['IPv4','TCP','172.16.2.2:5062']" remoteAddress="['IPv4','TCP','146.20.193.45:33441']"
ssl_error_reason="error:14094416:SSL routines:ssl3_read_bytes:sslv3 alert certificate unknown"
2017-09-19T11:12:09.721-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 15:12:09,721"
Module="network.tcp" Level="DEBUG": Src-ip="146.20.193.45" Src-port="33441" Dst-ip="172.16.2.2"
Dst-port="5062" Detail="TCP Connection Closed" Reason="Got EOF on socket"
```

Si vous analysez cela sous la perspective de Wireshark, vous verrez que l'Expressway-E présente son certificat. Si vous approfondissez votre étude du paquet, vous pourrez voir qu'uniquement le certificat du serveur est envoyé. Cisco Webex rejette ensuite cette prise de contact mutuelle de TLS en émettant un message d'erreur indiquant que l'autorité de certification est inconnue (Unknown CA), comme l'indique l'image.

Selected Packet

40	2017-09-19 15:12:09.610059	172.16.2.2	146.20.193.45	TLSv1.2	5062	33441	2600 Server hello, Certificate, Server Key Exchange, Certificate Request, Server hello Done
41	2017-09-19 15:12:09.664129	172.16.2.2	146.20.193.45	TLSv1.2	5062	33441	66 33441-5062 [ACK] Seq=201 Ack=1369 Win=17536 Len=0 TSval=3791983688 TSecr=360911709
42	2017-09-19 15:12:09.664330	146.20.193.45	172.16.2.2	TCP	33441	5062	66 33441-5062 [ACK] Seq=201 Ack=2535 Win=20480 Len=0 TSval=3791983688 TSecr=360911709
43	2017-09-19 15:12:09.664651	146.20.193.45	172.16.2.2	TCP	33441	5062	66 33441-5062 [ACK] Seq=201 Ack=2535 Win=20480 Len=0 TSval=3791983688 TSecr=360911709
44	2017-09-19 15:12:09.665670	146.20.193.45	172.16.2.2	TCP	33441	5062	78 [TCP Dup ACK 43#1] 33441-5062 [ACK] Seq=201 Ack=2535 Win=20480 Len=0 TSval=3791983707 TSecr=360911709
45	2017-09-19 15:12:09.721427	146.20.193.45	172.16.2.2	TLSv1.2	33441	5062	73 alert (Level: Fatal, Description: Certificate Unknown)
46	2017-09-19 15:12:09.721515	146.20.193.45	172.16.2.2	TCP	33441	5062	66 33441-5062 [FIN, ACK] Seq=208 Ack=2535 Win=20480 Len=0 TSval=3791983754 TSecr=360911744
47	2017-09-19 15:12:09.721758	172.16.2.2	146.20.193.45	TCP	5062	33441	66 5062-33441 [FIN, ACK] Seq=2385 Ack=209 Win=30080 Len=0 TSval=360911821 TSecr=3791983754
48	2017-09-19 15:12:09.731022	146.20.193.45	172.16.2.2	TCP	33441	5062	66 33441-5062 [ACK] Seq=209 Ack=2536 Win=20480 Len=0 TSval=3791983779 TSecr=360911821

Frame 40: 2600 bytes on wire (20800 bits), 2600 bytes captured (20800 bits) on interface 0

Ethernet II, Src: Vmware_S8:9f:31 (00:0c:29:58:9f:31), Dst: e0:0e:da:c8:8c:f3 (e0:0e:da:c8:8c:f3)

Internet Protocol Version 4, Src: 172.16.2.2 (172.16.2.2), Dst: 146.20.193.45 (146.20.193.45)

Transmission Control Protocol, Src Port: 5062 (5062), Dst Port: 33441 (33441), Seq: 1, Ack: 201, Len: 2534

Secure Sockets Layer

TLSv1.2 Record Layer: Handshake Protocol: Server hello

TLSv1.2 Record Layer: Handshake Protocol: Certificate

Content Type: Handshake (22)

Version: TLS 1.2 (0x0303)

Length: 1722

Handshake Protocol: Certificate

Handshake Type: Certificate (11)

Length: 1718

Certificates Length: 1715

Certificates (1715 bytes)

Certificate Length: 1712

Certificate (id-at-commonName=amer-expressway01.ciscotac.net,id-at-organizationalUnitName=domain control validated)

Signed Certificate

AlgorithmIdentifier (sha256withRSAEncryption)

Padding: 0

encrypted: 23238dab29a4d921bc432266e52faef0e8524bfb44129a7...

Spark Rejects the Handshake "Certificate Unknown" error

Expressway-E Server Certificate

Solution :

Afin de régler le problème dans ce cas, vous devez télécharger les CAS intermédiaires et racines qui sont engagées dans la signature du certificat d'Expressway-E dans le centre des certificats de CA de confiance (Trusted CA) :

- Étape 1. Ouvrez une session dans l'Expressway-E.
- Étape 2. Naviguez jusqu'à **Maintenance > Security > Trusted CA certificate**.
- Étape 3. Sélectionnez **Choose File** dans le menu Upload (Télécharger) situé en bas de l'interface utilisateur.
- Étape 4. Choisissez le certificat CA qui a été impliqué dans la signature de l'Expressway-E.
- Étape 5. Sélectionnez **Append CA Certificate** (ajouter le certificat de la CA).
- Étape 6. Répétez les étapes pour tous les certificats CA impliqués dans la signature du certificat Expressway-E (intermédiaire, racine).
- Étape 7. Sélectionnez **Append CA Certificate** (ajouter le certificat de la CA).

Une fois ce processus terminé, vous verrez que la chaîne entière de certificats faisant partie du processus de signature du certificat de serveur de l'Expressway-E est incluse dans l'échange de clés. Voici un exemple de ce que vous constaterez en analysant une capture de paquet au moyen de Wireshark.

Selected Packet

175	2017-09-20 14:22:13.336358	172.16.2.2	146.20.193.45	TLSv1.2	5062	48520	1426 Certificate
176	2017-09-20 14:22:13.354189	146.20.193.45	172.16.2.2	TCP	48520	5062	66 48520-5062 [ACK] Seq=201 Ack=1369 Win=17536 Len=0 TSval=3875387398 TSecr=444315436
177	2017-09-20 14:22:13.354815	146.20.193.45	172.16.2.2	TCP	48520	5062	66 48520-5062 [ACK] Seq=201 Ack=2737 Win=20480 Len=0 TSval=3875387398 TSecr=444315436
178	2017-09-20 14:22:13.355985	146.20.193.45	172.16.2.2	TCP	48520	5062	66 48520-5062 [ACK] Seq=201 Ack=4097 Win=23296 Len=0 TSval=3875387400 TSecr=444315436
179	2017-09-20 14:22:13.355999	172.16.2.2	146.20.193.45	TLSv1.2	5062	48520	715 Server Key Exchange
180	2017-09-20 14:22:13.366930	146.20.193.45	172.16.2.2	TCP	48520	5062	66 48520-5062 [ACK] Seq=201 Ack=4746 Win=26112 Len=0 TSval=3875387411 TSecr=444315455
197	2017-09-20 14:22:13.668592	146.20.193.45	172.16.2.2	TLSv1.2	48520	5062	73 alert (Level: Fatal, Description: Certificate unknown)
198	2017-09-20 14:22:13.668644	146.20.193.45	172.16.2.2	TCP	48520	5062	66 48520-5062 [FIN, ACK] Seq=208 Ack=4746 Win=26112 Len=0 TSval=3875387711 TSecr=444315455
199	2017-09-20 14:22:13.668871	172.16.2.2	146.20.193.45	TCP	5062	48520	66 5062-48520 [FIN, ACK] Seq=4746 Ack=209 Win=30080 Len=0 TSval=444315768 TSecr=3875387711
200	2017-09-20 14:22:13.681586	146.20.193.45	172.16.2.2	TCP	48520	5062	66 48520-5062 [ACK] Seq=209 Ack=4747 Win=26112 Len=0 TSval=3875387725 TSecr=444315768

Frame 175: 1426 bytes on wire (11408 bits), 1426 bytes captured (11408 bits) on interface 0

Ethernet II, Src: Vmware_S8:9f:31 (00:0c:29:58:9f:31), Dst: e0:0e:da:c8:8c:f3 (e0:0e:da:c8:8c:f3)

Internet Protocol Version 4, Src: 172.16.2.2 (172.16.2.2), Dst: 146.20.193.45 (146.20.193.45)

Transmission Control Protocol, Src Port: 5062 (5062), Dst Port: 48520 (48520), Seq: 2737, Ack: 201, Len: 1360

[2 Reassembled TCP Segments (3938 bytes): #174(2642), #175(1296)]

Secure Sockets Layer

TLSv1.2 Record Layer: Handshake Protocol: Certificate

Content Type: Handshake (22)

Version: TLS 1.2 (0x0303)

Length: 3933

Handshake Protocol: Certificate

Handshake Type: Certificate (11)

Length: 3929

Certificates Length: 3926

Certificates (3926 bytes)

Certificate Length: 1712

Certificate (id-at-commonName=amer-expressway01.ciscotac.net,id-at-organizationalUnitName=domain control validated)

Certificate Length: 1236

Certificate (id-at-commonName=Go Daddy Secure Certificate Authority - G2,id-at-organizationalUnitName=http://certs.godaddy.com/repository,id-at-organizationalUnitName=GoDaddy.com, Inc.,id-at-localityName=Scottsdale, id-at-stateOrProvinceName=Arizona,id-at-countryName=US)

Certificate Length: 969

Certificate (id-at-commonName=Go Daddy Root Certificate Authority - G2,id-at-organizationalUnitName=GoDaddy.com, Inc.,id-at-localityName=Scottsdale,id-at-stateOrProvinceName=Arizona,id-at-countryName=US)

Server

Intermediate

Root

Problème 4. Le pare-feu met fin à la prise de contact mutuelle de TLS

En règle générale, la solution Expressway s'interface avec un pare-feu. Dans bien des cas, le pare-feu en ligne lié à la solution exécute une sorte d'inspection de couche de l'application. Souvent avec la solution Expressway, lorsque le pare-feu exécute l'inspection de la couche

application, les administrateurs voient des résultats indésirables. Ce problème particulier vous permet de repérer les cas où une inspection de couche de l'application met fin abruptement à la connexion.

Au moyen des journaux de diagnostic de l'Expressway, vous pouvez chercher à consulter les tentatives de prises de contact mutuelles de TLS. Tel que nous l'avons signalé précédemment, ce processus de prise de contact devrait survenir peu de temps après l'établissement de la connexion TCP sur le port 5062. Dans ce cas, lorsque le pare-feu rompt la connexion, vous verrez ces erreurs dans les journaux de diagnostic.

```
Thread="0x7f6496669700": TTSSL_continueHandshake: Failed to establish SSL connection iResult="-1" error="5" bServer="false" localAddress="['IPv4','TCP','172.17.31.10:28351']"  
2017-06-13T13:31:38.760-05:00 vcse tvcs: Event="Outbound TLS Negotiation Error" Service="SIP"  
Src-ip="172.17.31.10" Src-port="28351" Dst-ip="198.101.251.5" Dst-port="5062" Detail="No SSL error available, probably remote disconnect" Protocol="TLS" Common-name="callservice.ciscopark.com" Level="1" UTCTime="2017-06-13 18:31:38,758"  
2017-06-13T13:31:38.760-05:00 vcse tvcs: UTCTime="2017-06-13 18:31:38,758" Module="network.tcp" Level="DEBUG": Src-ip="172.17.31.10" Src-port="28351" Dst-ip="198.101.251.5" Dst-port="5062" Detail="TCP Connection Closed" Reason="Got EOF on socket"
```

Sous la perspective de capture de paquets, vous verrez que l'Expressway-E présente son certificat à Cisco Webex. Vous voyez un RST de TCP provenant de Cisco Webex, comme l'illustre l'image.

The screenshot shows a network traffic capture in Wireshark. The top pane displays a list of packets. Packet 266 is selected, showing a TCP RST (Seq=6087, Ack=5998, Win=175104, Len=0) from 198.101.251.5 to 172.17.31.10. The middle pane shows the packet details for the selected packet, including the TLSv1.2 Record Layer and the Certificate. The certificate is a Go Daddy Root Certificate Authority. The bottom pane shows the certificate details, including the issuer and subject information.

Dans un premier temps, vous pourriez penser que quelque chose ne va pas avec le certificat d'Expressway-E. Afin de résoudre ce problème, vous devez tout d'abord déterminer les réponses à ces questions :

- Est-ce que l'Expressway-E porte la signature d'une autorité de certification publique réputée digne de confiance par Cisco Webex?
- Est-ce que le certificat Expressway-E et les éventuels autres certificats prenant part au processus de signature de l'Expressway-E ont été téléchargés manuellement dans le Cisco Webex Control Hub (<https://admin.ciscopark.com/>)?

Dans cette situation en particulier, la solution ne consistait pas à utiliser Cisco Webex Control Hub pour gérer les certificats Expressway-E. Cela signifie que le certificat de l'Expressway-E doit porter la signature d'une autorité de certification publique réputée digne de confiance par Cisco Webex. En cliquant sur le paquet du Certificat dans la capture de Wireshark (comme le montre l'illustration ci-dessous), vous pouvez voir que le certificat a bien été signé par une autorité de certification publique et que la chaîne entière de certificats a été envoyée à Cisco Webex. Par conséquent, le problème n'est probablement pas relié au certificat d'Expressway-E.

À ce stade, s'il est nécessaire d'isoler plus précisément la problématique, vous pourriez faire une capture de paquet de l'interface externe du pare-feu. Cependant, l'absence d'erreur de SSL dans le journal de diagnostic constitue un important point de données. Tel que nous l'avons abordé ci-dessus (Problème 3.) , *si Cisco Webex ne tient pas pour fiable le certificat d'Expressway-E, vous devriez voir un certain motif de déconnexion SSL*. Dans ce cas-ci, il n'y avait pas d'erreur SSL disponible.

Note: Si vous deviez obtenir une capture de paquets de l'interface externe du pare-feu, vous n'observeriez pas de RST de TCP provenant de l'environnement de Cisco Webex.

Solution

Pour cette solution en particulier, vous, en tant que partenaire ou client, devrez vous fier à votre équipe de sécurité. L'équipe devra vérifier si elle utilise une forme d'inspection de couche de l'application pour la solution Expressway et si c'est le cas, elle devra la désactiver. [L'Annexe 4 du guide de déploiement de VCS Control et Expressway explique pourquoi il est recommandé que les clients désactivent cette fonctionnalité.](#)

Problème 5. L'Expressway-E est signé par une autorité de certification publique, mais le concentrateur de contrôle Cisco Webex a d'autres certificats chargés

Cette situation en particulier se produit souvent lorsque vous avez déployé la solution d'Expressway en partant de rien et que vous n'avez pas au départ de certificat d'Expressway-E signé par une autorité de certification publique. Dans ce scénario, vous téléchargez le certificat du serveur Expressway-E (qui a été signé à l'interne) vers le Cisco Webex Control Hub afin que vous puissiez effectuer la prise de contact mutuelle avec succès. Par la suite, vous obtenez le certificat d'Expressway-E signé par une autorité de certification publique, toutefois vous oubliez de retirer le certificat du serveur du Cisco Webex Control Hub. Il est important de savoir que lorsqu'un certificat est téléchargé vers le Cisco Webex Control Hub, ce certificat l'emportera en priorité sur tout certificat ou toute chaîne que présente l'Expressway au cours de la prise de contact mutuelle de TLS.

Du point de vue de la journalisation de diagnostic d'Expressway-E, ce problème peut ressembler à la signature de journalisation qui est rencontrée lorsque Cisco Webex ne fait pas confiance au certificat Expressway-E, par exemple dans le cas où l'Expressway-E n'envoie pas sa chaîne complète ou le certificat Expressway-E n'est pas signé par une autorité de certification publique de confiance de Cisco Webex. Ci-dessous, un exemple de ce que vous pouvez constater dans la journalisation d'Expressway-E s'attachant à la prise de contact mutuelle de TLS :

```
2017-09-20T10:22:13.669-04:00 amer-expressway01 tvcs: Event="Inbound TLS Negotiation Error"
Service="SIP" Src-ip="146.20.193.45" Src-port="48520" Dst-ip="172.16.2.2" Dst-port="5062"
Detail="sslv3 alert certificate unknown" Protocol="TLS" Level="1" UTCTime="2017-09-20
14:22:13,668"
2017-09-20T10:22:13.669-04:00 amer-expressway01 tvcs: UTCTime="2017-09-20 14:22:13,668"
Module="developer.ssl" Level="ERROR" CodeLocation="ppcmains/ssl/ttssl/ttssl_openssl.cpp(68)"
Method="::TTSSLSErrorOutput" Thread="0x7f4a2c16f700": TTSSL_continueHandshake: Failed to
establish SSL connection iResult="0" error="1" bServer="true"
localAddress="['IPv4','TCP','172.16.2.2:5062']" remoteAddress="['IPv4','TCP','146.20.193.45:48520']"
ssl_error_reason="error:14094416:SSL routines:ssl3_read_bytes:sslv3 alert certificate unknown"
2017-09-20T10:22:13.669-04:00 amer-expressway01 tvcs: UTCTime="2017-09-20 14:22:13,668"
Module="network.tcp" Level="DEBUG": Src-ip="146.20.193.45" Src-port="48520" Dst-ip="172.16.2.2"
Dst-port="5062" Detail="TCP Connection Closed" Reason="Got EOF on socket"
```


En y jetant un œil du point de vue de Wireshark, vous pourrez constater qu'Expressway-E présente son certificat dans l'élément de la ligne 175. Quelques lignes plus bas, l'environnement de Cisco Webex rejette le certificat en émettant une erreur de certificat inconnu (Certificate Unknown error), comme l'indique l'image.

Selected Packet

Spark sends a "Certificate Unknown" Error

Server
Intermediate
Root

Si vous sélectionnez le paquet de certificat envoyé par l'Expressway-E, vous pouvez développer les renseignements sur le certificat pour déterminer si l'Expressway-E

1. porte la signature d'une [autorité de certification publique que Cisco Webex tient pour fiable](#)
2. et s'il inclut la chaîne complète de certificats dans la signature.

Dans cette situation, les deux critères sont satisfaits. Cela fait penser qu'il n'y a aucun problème avec le certificat d'Expressway-E.

Solution

Étape 1. Connectez-vous au [Cisco Webex Control Hub](#).

Étape 2. Sélectionnez **Services** dans le volet gauche.

Étape 3. Sélectionnez **Paramètres** sous la carte d'appel hybride.

Étape 4. Faites défiler jusqu'à la section Call Service Connect et recherchez les certificats pour les appels SIP chiffrés pour voir si des certificats indésirables sont répertoriés. Dans un tel cas, cliquez sur l'icône de poubelle à côté du certificat.

Étape 5. Sélectionnez **Supprimer**.

Note: Il est important que l'analyse soit effectuée et il est déterminé que le client n'utilise pas les certificats téléchargés dans Webex Control Hub avant de les retirer.

Pour plus de renseignements à propos du téléchargement de votre certificat Expressway-E dans le Cisco Webex Control Hub, vérifiez [la section du guide de déploiement Hybrid Call](#).

Problème 6. Expressway ne mappe pas l'appel entrant à la zone DNS hybride Cisco Webex

La fonctionnalité de mise en correspondance de TLS d'appels entrants fonctionne en conjonction

avec le nom de sujet de vérification (Verify Subject Name) de TLS. Ces deux éléments sont configurés dans la zone DNS d'Hybrid Call. Ce scénario présente les problèmes et les défis observés avec l'Expressway avant x12.5. Dans x12 et les versions ultérieures, un nouveau type de zone a été mis en oeuvre appelé la zone « Webex ». Cette zone préremplit toutes les configurations requises pour l'intégration avec Webex. Si vous exécutez x12.5 et déployez Webex Hybrid Call, il est recommandé d'utiliser le type de zone **Webex** afin que le domaine des services d'appel hybrides (callservice.webex.com) soit configuré automatiquement pour vous. Cette valeur correspond au nom secondaire du sujet du certificat Webex qui est présenté lors de la connexion mutuelle TLS et permet à la connexion et au mappage entrant vers l'Expressway de réussir.

Si vous utilisez une version de code sous x12.5 ou si vous n'utilisez pas la zone Webex, vous voudrez poursuivre avec l'explication ci-dessous qui montre comment identifier et corriger les problèmes où l'Expressway ne mappe pas l'appel entrant vers la zone DNS hybride Webex.

La fonctionnalité conduit à un processus en trois étapes :

1. Expressway-E accepte le certificat de Cisco Webex.
2. Expressway-E examine le certificat de Cisco Webex pour déterminer s'il y a un autre nom de sujet (Subject Alternate Name) qui correspond au nom de sujet de vérification de TLS : callservice.ciscopark.com.
3. Expressway-E met en correspondance la connexion entrante au moyen de la zone DNS de Cisco Webex Hybrid.

Si l'authentification n'a pas réussi, cela signifie que la validation du certificat a échoué. L'appel entre dans la zone par défaut et est acheminé selon les règles de recherche précisées pour les scénarios d'une entreprise à l'autre (business-to-business), si l'option business-to-business est configurée sur Expressway-E.

Comme dans les autres scénarios, vous devez utiliser la journalisation de diagnostic et les captures de paquets pour déterminer l'aspect que prend l'échec, puis utiliser la capture de paquets pour déterminer quel côté envoie le RST. Voici un exemple de la connexion de TCP qui fait l'objet de tentatives avant d'être établie.

```
2017-09-22T10:09:56.471-04:00 amer-expressway01 tvcs: UTCTime="2017-09-22 14:09:56,471"
Module="network.tcp" Level="DEBUG": Src-ip="148.62.40.52" Src-port="44205" Dst-ip="172.16.2.2"
Dst-port="5062" Detail="TCP Connecting"
2017-09-22T10:09:56.471-04:00 amer-expressway01 tvcs: UTCTime="2017-09-22 14:09:56,471"
Module="network.tcp" Level="DEBUG": Src-ip="148.62.40.52" Src-port="44205" Dst-ip="172.16.2.2"
Dst-port="5062" Detail="TCP Connection Established"
```

Maintenant que la connexion de TCP est établie, la prise de contact mutuelle de TLS peut suivre. Vous pouvez observer que peu de temps après la mise en application de la prise de contact mutuelle, le processus est rapidement interrompu pour cause d'erreur.

```
2017-09-22T10:09:57.044-04:00 amer-expressway01 tvcs: UTCTime="2017-09-22 14:09:57,044"
Module="developer.ssl" Level="INFO" CodeLocation="ppcmains/ssl/ttssl/ttssl_openssl.cpp(1974) "
Method="::ttssl_continueHandshake" Thread="0x7f044e7cc700": Detail="Handshake in progress"
Reason="want read/write"
2017-09-22T10:09:57.123-04:00 amer-expressway01 tvcs: Event="Inbound TLS Negotiation Error"
Service="SIP" Src-ip="148.62.40.52" Src-port="44205" Dst-ip="172.16.2.2" Dst-port="5062"
Detail="Peer's TLS certificate identity was unacceptable" Protocol="TLS" Level="1"
UTCTime="2017-09-22 14:09:57,123"
2017-09-22T10:09:57.123-04:00 amer-expressway01 tvcs: UTCTime="2017-09-22 14:09:57,123"
Module="network.tcp" Level="DEBUG": Src-ip="148.62.40.52" Src-port="44205" Dst-ip="172.16.2.2"
Dst-port="5062" Detail="TCP Connection Closed" Reason="Peer's TLS certificate identity was
```


unacceptable"

Examinez cette situation sous l'angle de pcap, et vous pourrez vous faire une meilleure idée de

- qui émet le RST
- et quels sont les certificats transmis, pour vérifier s'ils sont corrects.

Lorsque vous analysez cette capture en particulier, vous pouvez voir que l'Expressway-E envoie le RST. Lorsque vous consultez le certificat de Cisco Webex qui est transmis, vous observez aussi que la chaîne complète est envoyée. De plus, selon le message d'erreur dans le journal de diagnostic, vous pouvez conclure que le scénario selon lequel l'Expressway-E ne tient pas pour fiables les CA publiques de Cisco Webex n'est pas en cause. Sinon, vous auriez vu une erreur comme la suivante « **self signed certificate in certificate chain** » (signalant le certificat autosigné dans la chaîne de certificats). Vous pouvez approfondir votre examen des détails de paquets, comme l'indique l'image.

The screenshot shows a Wireshark network capture. The top pane displays a list of packets. Packet 70 is highlighted in red, indicating a TCP segment with a RST flag. The details pane for packet 70 shows the following information:

- Frame 62: 294 bytes on wire (2352 bits), 294 bytes captured (2352 bits)
- Ethernet II, Src: e0:0e:da:c8:8c:f3 (e0:0e:da:c8:8c:f3), Dst: vmware_58:9f:31 (00:0c:29:58:9f:31)
- Internet Protocol Version 4, Src: 148.62.40.52 (148.62.40.52), Dst: 172.16.2.2 (172.16.2.2)
- Transmission Control Protocol, Src Port: 44205 (44205), Dst Port: 5062 (5062), Seq: 5673, Ack: 4746, Len: 228
- [5 Reassembled TCP segments (5700 bytes): #54(1368), #56(1368), #59(1368), #60(1368), #62(228)]
- Secure Sockets Layer
 - TLSv1.2 Record Layer: Handshake Protocol: Multiple Handshake Messages
 - Content Type: Handshake (22)
 - Version: TLS 1.2 (0x0303)
 - Length: 5695
 - Handshake Protocol: Certificate
 - Handshake Type: Certificate (11)
 - Length: 5553
 - Certificates Length: 5550
 - Certificates (5550 bytes)
 - Certificate Length: 2338
 - Certificate (id-at-commonName=l2sip-cfa-01.ciscospark.com,id-at-organizationName=Cisco Systems, Inc.,id-at-localityName=San Jose,id-at-stateOrProvinceName=CA,id-at-countryName=US)
 - Certificate Length: 1736
 - Certificate (id-at-commonName=HydrantID SSL ICA G2,id-at-organizationName=HydrantID (Avalanche Cloud Corporation),id-at-countryName=US)
 - Certificate Length: 1467
 - Certificate (id-at-commonName=Quovadis Root CA 2,id-at-organizationName=Quovadis Limited,id-at-countryName=BM)
 - Handshake Protocol: Client Key Exchange

Si vous cliquez sur le certificat du serveur Webex et faites afficher de plus amples renseignements pour voir les autres noms du sujet, c.-à-d. les Subject Alternate Names (dnsName), vous pouvez vérifier que **callservice.ciscospark.com** est indiqué.

Naviguez jusqu'à Wireshark : **Certificate > Extension > General Names > GeneralName > dnsName : callservice.ciscospark.com**

Cela confirme entièrement que le certificat de Webex semble parfaitement correct.

Vous pouvez maintenant confirmer que le nom de sujet de vérification de TLS (TLS Verify Subject Name) est correct. Tel que signalé précédemment, si vous avez xConfiguration, vous pouvez consulter la section de configuration de la zone pour déterminer comment le nom de sujet de vérification de TLS a été configuré. Pour xConfiguration, il convient de signaler que les zones sont présentées en ordre, la Zone 1 en premier. Voici une xConfiguration provenant de l'environnement problématique analysé ci-dessus. De toute évidence, le nom de sujet de vérification de TLS ne pose pas de problème.

```
*c xConfiguration Zones Zone 6 DNS SIP TLS Verify Mode: "On"
```

```
*c xConfiguration Zones Zone 6 DNS SIP TLS Verify Subject Name: "callservice.ciscospark.com"
```

La prochaine chose à examiner est la mise en correspondance des données entrantes de vérification de TLS (**TLS verify inbound mapping**). Cela vous permet de confirmer que votre mise en correspondance de la connexion TLS dans la zone DNS de Webex Hybrid est correcte. Il est aussi possible de tirer parti de xConfiguration pour analyser cela. Dans la xConfiguration, la mise

en correspondance des données entrantes de vérification de TLS **TLS verify inbound mapping s'appelle DNS ZIP TLS Verify InboundClassification**. Comme vous pouvez le voir dans cet exemple, la valeur est réglée à « Off » (arrêt).

```
*c xConfiguration Zones Zone 6 DNS SIP TLS Verify InboundClassification: "Off"
```

```
*c xConfiguration Zones Zone 6 Name: "Hybrid Call Services DNS"
```

Étant donné que la valeur est réglée à « Off » (arrêt), cela signifie que le VCS ne peut pas tenter de mettre en correspondance des données entrantes de connexion de TLS dans cette zone. L'appel entre donc dans la zone par défaut et vérifié est acheminé selon les règles de recherche précisées pour les scénarios d'une entreprise à l'autre (business-to-business), si l'option business-to-business est configurée sur Expressway-E.

Solution

Afin d'aborder cette situation, vous devez définir la mise en correspondance de données entrantes de vérification de TLS en sélectionnant « On » (mise en marche) pour la zone DNS d'Hybrid Call. Voici les étapes à suivre pour le faire.

1. Ouvrez une session dans l'Expressway-E
2. Naviguez jusqu'à **Configuration > Zones > Zones**
3. Sélectionnez **Hybrid Call DNS Zone**
4. Pour **TLS verify inbound mapping**, choisissez **On**
5. Sélectionnez **Save (enregistrer)**

Note: Reportez-vous à la pour connaître le comportement de journalisation de base. Cette section présente la vérification du certificat s'exécutant sur Expressway, de même que la mise en correspondance des données de la zone DNS de Webex Hybrid.

Problème 7. Expressway-E utilise un certificat auto-signé par défaut

Dans certains nouveaux déploiements de Hybrid Call Service Connect, la signature du certificat Expressway-E est oubliée, ou encore, on pense que le certificat de serveur par défaut peut être utilisé. Certaines personnes pensent que c'est possible parce que Cisco Webex Control Hub vous permet de charger un certificat personnalisé sur le portail. (**Services > Settings (sous Hybrid Call card) > Upload (sous Certificates for Encrypted Calls)**)

Si vous portez attention aux énoncés au sujet des **Certificates for Encrypted SIP Calls**, vous **observerez la directive suivante** : « Use certificates provided from the Cisco Collaboration default trust list or upload your own. If you use your own, ensure the hostnames are on a verified domain ». Cela signifie : utilisez des certificats provenant de la liste de confiance par défaut de Cisco Collaboration ou encore, téléchargez les vôtres. Si vous utilisez les vôtres, assurez-vous que les noms d'hôte proviennent d'un domaine vérifié. L'élément clé de la directive est le suivant : **« assurez-vous que les noms d'hôte proviennent d'un domaine vérifié. »**

Lorsque vous faites du dépannage pour un problème qui correspond à cette situation, n'oubliez pas que les symptômes dépendront de l'orientation de l'appel. Si l'appel provient d'un téléphone sur place, vous pouvez vous attendre à ce que l'application Cisco Webex ne sonne pas. De même, si vous essayez de retracer l'appel à partir de l'historique de recherche Expressways, vous constaterez que l'appel s'est rendu sur l'Expressway-E et s'est arrêté là. Si l'appel provient d'une application de Cisco Webex et était destiné à un site sur place, le téléphone sur place ne sonne pas. Dans un tel cas, l'historique de recherche d'Expressway-E et d'Expressway-C ne révélera

rien.

Dans ce scénario en particulier, l'appel provenait d'un téléphone sur place. Au moyen de l'historique de recherche d'Expressway-E, vous pouvez déterminer que l'appel s'est rendu au serveur. À ce stade, vous pouvez examiner de plus près la journalisation de diagnostic pour déterminer ce qui est arrivé. Pour commencer cette analyse, dans un premier temps, vérifiez si une connexion de TCP a été tentée et établie sur le port 5062. Au moyen d'une recherche dans les journaux de diagnostic d'Expressway-E pour les traces de la connexion TCP (« TCP Connecting »), en particulier une recherche pour les lignes portant la balise « Dst-port=5062 », vous pouvez déterminer si la connexion a été établie.

```
2017-09-26T08:18:08.428-04:00 amer-expressway01 tvcs: UTCTime="2017-09-26 12:18:08,426"
Module="network.tcp" Level="DEBUG": Src-ip="146.20.193.45" Src-port="59720" Dst-ip="172.16.2.2"
Dst-port="5062" Detail="TCP Connecting"
2017-09-26T08:18:08.428-04:00 amer-expressway01 tvcs: UTCTime="2017-09-26 12:18:08,426"
Module="network.tcp" Level="DEBUG": Src-ip="146.20.193.45" Src-port="59720" Dst-ip="172.16.2.2"
Dst-port="5062" Detail="TCP Connection Established"
```

Maintenant que vous avez confirmé que la connexion de TCP est établie, vous pouvez analyser la prise de contact mutuelle de TLS qui s'est produite immédiatement après. Comme vous pouvez le voir dans l'extrait ici, la prise de contact mutuelle échoue et le certificat est inconnu (« **sslv3 alertcertificate unknown** »)

```
2017-09-26T08:18:08.441-04:00 amer-expressway01 tvcs: UTCTime="2017-09-26 12:18:08,441"
Module="developer.ssl" Level="INFO" CodeLocation="ppcmains/ssl/ttssl/ttssl_openssl.cpp(1974)"
Method="::ttssl_continueHandshake" Thread="0x7f930adab700": Detail="Handshake in progress"
Reason="want read/write"
2017-09-26T08:18:08.455-04:00 amer-expressway01 tvcs: Event="Inbound TLS Negotiation Error"
Service="SIP" Src-ip="146.20.193.45" Src-port="59720" Dst-ip="172.16.2.2" Dst-port="5062"
Detail="sslv3 alert certificate unknown" Protocol="TLS" Level="1" UTCTime="2017-09-26
12:18:08,455"
2017-09-26T08:18:08.455-04:00 amer-expressway01 tvcs: UTCTime="2017-09-26 12:18:08,455"
Module="developer.ssl" Level="DEBUG" CodeLocation="ppcmains/ssl/ttssl/ttssl_openssl.cpp(1997)"
Method="::ttssl_continueHandshake" Thread="0x7f930adab700": Detail="Handshake Failed"
Reason="want error ssl"
2017-09-26T08:18:08.455-04:00 amer-expressway01 tvcs: UTCTime="2017-09-26 12:18:08,455"
Module="developer.ssl" Level="ERROR" CodeLocation="ppcmains/ssl/ttssl/ttssl_openssl.cpp(68)"
Method="::TTSSLErrorOutput" Thread="0x7f930adab700": TTSSL_continueHandshake: Failed to
establish SSL connection iResult="0" error="1" bServer="true"
localAddress="['IPv4','TCP','172.16.2.2:5062']" remoteAddress="['IPv4','TCP','146.20.193.45:59720']"
ssl_error_reason="error:14094416:SSL routines:ssl3_read_bytes:sslv3 alert certificate unknown"
2017-09-26T08:18:08.455-04:00 amer-expressway01 tvcs: UTCTime="2017-09-26 12:18:08,455"
Module="network.tcp" Level="DEBUG": Src-ip="146.20.193.45" Src-port="59720" Dst-ip="172.16.2.2"
Dst-port="5062" Detail="TCP Connection Closed" Reason="Got EOF on socket"
```

À l'examen de la capture de paquets découlant de la journalisation de diagnostic Expressway-E, vous pouvez voir que l'erreur de certificat inconnu proviendrait de Cisco Webex, comme l'indique l'image.

No.	Time	Source	Destination	Protocol	S Port	D Port	Length	Info
3	2017-09-26 12:18:08.415918	146.20.193.45	172.16.2.2	TCP	59720	5062	74	59720->5062 [SYN] Seq=0 win=14600 Len=0 MSS=1380 SACK_PERM=1 TSval=91375166 TSecr=0
4	2017-09-26 12:18:08.415941	172.16.2.2	146.20.193.45	TCP	5062	59720	74	5062->59720 [SYN, ACK] Seq=0 Ack=1 win=28860 Len=0 MSS=1460 SACK_PERM=1 TSval=95527051
5	2017-09-26 12:18:08.426317	146.20.193.45	172.16.2.2	TCP	59720	5062	66	59720->5062 [ACK] Seq=1 Ack=1 win=14720 Len=0 TSval=91375177 TSecr=955270515
6	2017-09-26 12:18:08.427715	146.20.193.45	172.16.2.2	TLSv1.2	59720	5062	266	client Hello
7	2017-09-26 12:18:08.427728	172.16.2.2	146.20.193.45	TCP	5062	59720	66	5062->59720 [ACK] Seq=1 Ack=201 win=30080 Len=0 TSval=955270527 TSecr=91375178
8	2017-09-26 12:18:08.440978	172.16.2.2	146.20.193.45	TLSv1.2	5062	59720	1780	Server Hello, Certificate, Server Key Exchange, Certificate Request, Server Hello Do
9	2017-09-26 12:18:08.453269	146.20.193.45	172.16.2.2	TCP	59720	5062	66	59720->5062 [ACK] Seq=201 Ack=1369 win=17536 Len=0 TSval=91375204 TSecr=955270540
10	2017-09-26 12:18:08.453308	146.20.193.45	172.16.2.2	TCP	59720	5062	66	59720->5062 [ACK] Seq=201 Ack=1715 win=20352 Len=0 TSval=91375204 TSecr=955270540
11	2017-09-26 12:18:08.455698	146.20.193.45	172.16.2.2	TLSv1.2	59720	5062	73	Alert (Level: Fatal), Description: certificate unknown

Si vous inspectez le certificat du serveur par défaut (Default Server certificate) de l'Expressway-E,

vous pouvez voir que le « Common Name » (nom courant) et les « Subject Alternate Names » (autres noms de sujet) ne comprend pas de domaine vérifié (« Verified Domain ») (**rtp.ciscotac.net**). Vous avez ensuite des données probantes sur ce qui cause ce problème, comme l'indique l'image.

À ce stade, vous avez déterminé que le certificat du serveur Expressway-E doit être signé par une autorité de certification (CA) publique ou une autorité de certification (CA) interne.

Solution

Afin de résoudre ce problème, vous avez deux options :

1. Veiller à ce que le certificat de l'Expressway-E porte la signature d'une [CA publique réputée digne de confiance par Cisco Webex](#).

Ouvrez une session dans l'Expressway. Naviguez jusqu'à **Maintenance > Security > Server certificate**. Sélectionnez **Generate CSR** (produire CSR). Saisissez les informations de certificat requis et vous assurer que le **Supplémentaires noms autre champ** contient le **Vérifié Domaine** décrites dans le **Concentrateur de Contrôle Webex**. Cliquez sur **Generate CSR**. Fournir le CSR à la tierce autorité de certification publique pour signature. Lorsque le certificat sera de retour, naviguez jusqu'à **Maintenance > Security > Server certificates**. Dans la section **Upload New Certificate (télécharger le nouveau certificat)** à côté de **Select the server certificate file** (sélectionner le fichier de certificat du serveur), sélectionnez **Choose File (choisir un fichier)** puis sélectionnez **signed certificate** (certificat signé). Sélectionnez **Upload server certificate data** (télécharger les données de certificat de serveur). Naviguez jusqu'à **Maintenance > Security > Trusted CA certificate**. Dans la section **Upload** (télécharger) à côté de **Select the file containing trusted CA certificates** (sélectionner le fichier qui renferme les certificats de CA de confiance), sélectionnez **Choose File** (choisir un fichier). Sélectionnez n'importe quel des certificats racines et intermédiaires provenant de l'autorité de certification publique. Sélectionnez **Append CA Certificate** (ajouter le certificat de la CA). Redémarrez l'Expressway-E.

2. Veillez à ce que le certificat d'Expressway-E soit signé par une autorité de certification (CA)

interne, puis téléversez l'Expressway-E et l'autorité de certification (CA) interne dans Cisco Webex Control Hub.

Ouvrez une session dans l'Expressway. Naviguez jusqu'à **Maintenance > Security > Server certificate**. Sélectionnez **Generate CSR (produire CSR)**. Saisissez les renseignements de certificat requis et vérifiez que le *Additional alternative names field comprend le domaine vérifié (Verified Domain)* décrit dans le Webex Control Hub. Cliquez sur **Generate CSR**. Fournir le CSR à la tierce autorité de certification publique pour signature. Au retour du certificat, Accédez à **Maintenance > Sécurité > certificats Serveur**. Dans la section **Upload New Certificate (télécharger le nouveau certificat)** à côté de **Select the server certificate file** (sélectionner le fichier de certificat du serveur), sélectionnez **Choose File (choisir un fichier)** puis sélectionnez **signed certificat (certificat signé)**. Sélectionnez **Upload server certificate data (télécharger les données de certificat de serveur)**. Naviguez jusqu'à **Maintenance > Security > Trusted CA certificate**. Dans la section **Upload (télécharger)** à côté de **Select the file containing trusted CA certificates (sélectionner le fichier qui renferme les certificats de CA de confiance)**, sélectionnez **Choose File (choisir un fichier)**. Sélectionnez n'importe quel des certificats racines et intermédiaires provenant de l'autorité de certification publique. Sélectionnez **Append CA Certificate (ajouter le certificat de la CA)**. Redémarrez l'Expressway-E.

2a. Téléversez le certificat de l'autorité de certification interne et d'Expressway-E dans Cisco Webex Control Hub.

1. Connectez-vous au [Cisco Webex Control Hub](#) en tant qu'administrateur.
2. Sélectionnez **Services**.
3. Sélectionnez **Paramètres** sous la carte Hybrid Call Service.
4. Dans la section des certificats des appels SIP chiffrés (**Certificates for Encrypted SIP Calls section**) sélectionnez **Upload (télécharger)**.
5. Sélectionnez les certificats CA interne et Expressway-E.

Entrant : Cisco Webex vers le site

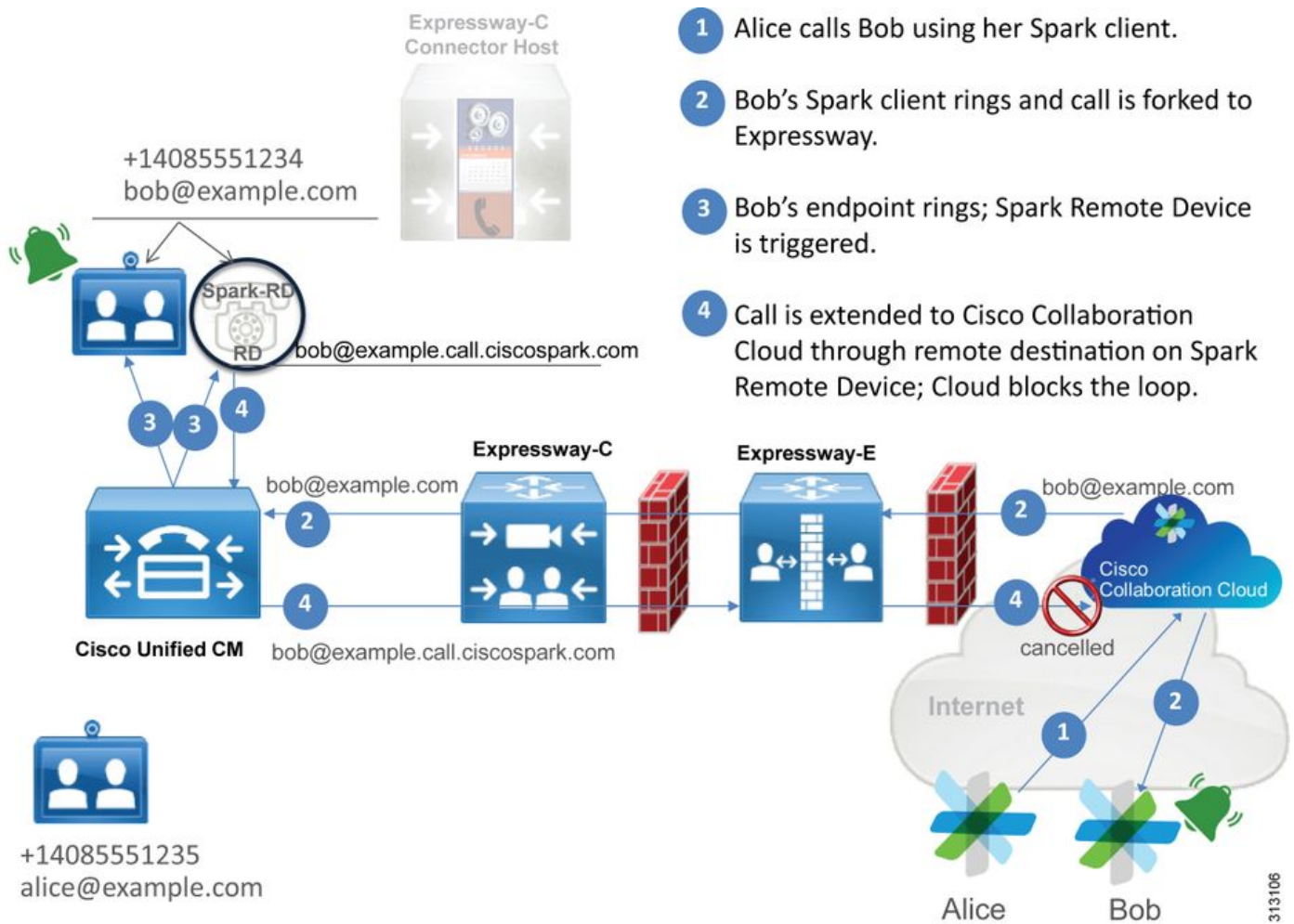
Presque tous les échecs d'une communication de Cisco Webex vers un site entraînent les mêmes symptômes déclarés : « Lorsque j'appelle de l'application de mon Cisco Webex à l'application d'un collègue, son application sonne, mais le téléphone sur le site ne sonne pas. » Afin de résoudre ce genre de problématique, vous trouverez utile de comprendre les flux d'appels et la logique s'appliquant lorsque ce genre d'appel s'effectue.

Flux logique de haut niveau

1. L'appelant de l'application de Cisco Webex lance l'appel.
2. L'application de l'appelé sonne.
3. L'appel est acheminé par l'environnement de Cisco Webex
4. L'environnement de Cisco Webex doit effectuer une recherche de DNS en fonction de la destination SIP configurée du client dans le Cisco Webex Control Hub
5. L'environnement de Cisco Webex tente de se connecter à l'Expressway sur le port 5062
6. L'environnement de Cisco Webex tente d'effectuer une prise de contact mutuelle de TLS
7. L'environnement de Cisco Webex envoie une invitation (INVITE) SIP à Expressway.
L'invitation est transmise au point terminal de collaboration/téléphone IP sur place.
8. Cisco Webex et l'entreprise complètent la négociation de SIP
9. Cisco Webex et l'entreprise commencent à envoyer et recevoir des communications.

Flux d'appels

Naviguez jusqu'à Cisco Webex app > Cisco Webex environment > Expressway-E > Expressway-C > On-Premises Collaboration Endpoint/IP Phone, comme l'indique l'image.



Voici quelques-uns des problèmes courants observés dans l'infrastructure sur place au sujet des appels entrants provenant de Webex.

Problème 1. Cisco Webex ne peut pas résoudre le SRV/nom d'hôte DNS de l'Expressway-E

Lorsque l'on examine le flux d'appels de Cisco Webex vers les sites sur place, la première étape logique que franchit Cisco Webex consiste à vérifier comment communiquer avec l'Expressway sur place. Comme il en est question ci-haut, Cisco Webex va tenter de se connecter à l'Expressway sur place en effectuant une recherche de SRV fondée sur la configuration de la destination SIP qui est affichée dans la [page de paramètres Hybrid Call Service Settings dans le Cisco Webex Control Hub](#).

Si vous tentez de faire un dépannage dans cette situation sous une perspective de journal de diagnostic Expressway-E, vous ne verrez pas le trafic en provenance de Cisco Webex. Si vous tentez de faire des recherches de connexion TCP, vous n'observerez pas Dst-port=5062 ou les processus subséquents de prise de contact mutuelle de MTLS ou d'invitation SIP provenant de Cisco Webex.

S'il s'agit de votre situation, vous devrez vérifier comment la **SIP Destination a été configurée dans Cisco Webex Control Hub**. Vous pouvez également utiliser l'outil **Hybrid Connectivity Test Tool pour vérifier la connectivité dans le cadre de vos efforts de dépannage**. Cet outil (Hybrid Connectivity Test Tool) vérifie s'il y a une adresse DNS valide, si Cisco Webex peut se connecter

au port renvoyé dans la recherche de SRV et si l'Expressway sur place a un certificat valide auquel Cisco Webex peut se fier.

1. Ouvrez une session dans le Cisco Webex Control Hub
2. Sélectionnez les Services
3. Sélectionnez le lien conduisant aux paramètres (Settings) dans la carte Call card d'Hybrid.
4. Dans la section Call Service Connect, vérifiez le domaine utilisé pour l'adresse publique de SRV de SIP le champ Destination du SIP.
5. Si l'enregistrement est saisi correctement, cliquez sur **Test pour voir si l'enregistrement est valide**.
6. Comme le montre l'illustration ci-dessous, vous pouvez voir clairement que le domaine public n'a pas un enregistrement SRV de SIP correspondant connexe, tel que l'indique l'image.

SIP Destination ⓘ

mtls.rtp.ciscotac.net

Test

Save

✖ Your SIP Destination is not configured correctly. [View test results](#)

Sélectionnez **View test results (afficher les résultats de test)** pour consulter de plus amples renseignements au sujet de ce qui a échoué, comme l'illustre l'image.

Verify SIP Destination

DNS Lookup failed. Check that a DNS or SRV record exists for your SIP Destination and that it resolves to one or more valid IP addresses.

Vous pouvez aussi recourir à une autre approche, qui consiste à faire une recherche d'enregistrement SRV en utilisant nslookup. Voici les commandes que vous pouvez exécuter pour vérifier si la destination SIP existe.

```
C:\Users\pstoiano>nslookup
> server 8.8.8.8
Default Server: google-public-dns-a.google.com
Address: 8.8.8.8
> set type=SRV
> _sips._tcp.mtls.rtp.ciscotac.net
Server: google-public-dns-a.google.com
Address: 8.8.8.8
DNS request timed out.
timeout was 2 seconds.
DNS request timed out.
timeout was 2 seconds.
*** Request to google-public-dns-a.google.com timed-out
```

Comme vous pouvez le constater dans le bloc de codes ci-dessus, la commande nslookup a été lancée, puis le serveur s'est réglé à 8.8.8.8, ce qui correspond à un serveur DNS public de Google. En dernier lieu, vous définissez les types d'enregistrement pour faire une recherche d'enregistrements SRV. À ce stade-ci, vous pourrez ensuite émettre l'enregistrement SRV complet que vous souhaitez consulter. En fin de compte, il y aura un arrêt automatique

s'appliquant aux demandes.

Solution

1. Configurez une adresse SRV de SIP publique pour l'Expressway-E sur le site utilisé pour héberger les noms de domaine public.
2. Configurez un nom d'hôte qui permettra de remédier aux problèmes d'adresse IP de l'Expressway-E
3. Configurez la destination SIP pour afficher le domaine utilisé pour l'adresse SRV de SIP créée à l'Étape 1. Ouvrez une session dans le [Cisco Webex Control Hub](#) Sélectionner **des services** Sélectionnez le lien conduisant aux paramètres (**Settings**) dans la carte *Hybrid Call card* Dans la section Call Service Connect, saisissez le domaine utilisé pour l'adresse publique SRV de SIP dans le **champ SIP Destination**. Sélectionnez Save (enregistrer)

Note: Si l'enregistrement SRV du SIP que vous souhaitez utiliser est déjà utilisé pour les communications « business-to-business », nous vous recommandons de préciser un sous-domaine du domaine d'entreprise comme adresse de découverte SIP de Cisco Webex Control Hub et par conséquent, un enregistrement public SRV de DNS, comme suit :

Service and protocol (service et protocole) : `_sips._tcp.mtls.example.com`

Priorité : 1

Weight (poids) : 10

Port number (numéro de port) : 5062

Target (cible) : `us-expe1.example.com`

La recommandation ci-dessus provient directement du [guide de conception de Cisco Webex Hybrid Design](#).

Solution de rechange

Si le client n'a pas un enregistrement SIP de SRV (et ne prévoit pas en créer un), il peut aussi afficher l'adresse IP publique d'Expressway portant le suffixe : « : 5062 ». À la suite de cette action, l'environnement de Webex ne tentera pas une recherche de SRV, mais se connectera plutôt à `%Expressway_Pub_IP%:5062`. (Par exemple : `64.102.241.236:5062`)

1. Configurez la destination SIP pour qu'elle soit formatée comme suit `%Expressway_Pub_IP%:5062`. (Exemple : `64.102.241.236:5062`) Ouvrez une session dans le [Cisco Webex Control Hub](#) Sélectionner **des services** Sélectionnez le lien conduisant aux paramètres (**Settings**) dans la carte *Hybrid Call card* Dans la section Call Service Connect, saisissez `%Expressway_Pub_IP%:5062` dans le **champ SIP Destination**. Sélectionnez Save (enregistrer)

Pour en savoir plus sur l'adresse de la destination du SIP ou sur l'enregistrement SRV à configurer. Consultez la section [Enable Hybrid Call Service Connect for Your Organization du guide de déploiement des services Hybrid Call de Cisco Webex ou encore, le guide de conception de Cisco Webex Hybrid Design](#).

Problème 2. Échec du socket : Port 5062 est bloqué à l'entrée d'Expressway

Après la résolution DNS, l'environnement de Cisco Webex tentera d'établir une connexion TCP sur le port 5062 à l'adresse IP qui a été retournée au cours de la recherche de DNS. Cette

adresse IP est l'adresse IP publique provenant de l'Expressway-E sur place. Si l'environnement de Cisco Webex est incapable d'établir cette connexion TCP, l'appel entrant sur place échouera ensuite. Le symptôme révélant ce problème en particulier est le même que presque tous les autres échecs liés à un appel entrant de Cisco Webex : le téléphone sur place ne sonne pas.

Si vous faites un dépannage pour ce problème au moyen des journaux de diagnostic Expressway, vous ne verrez pas de trafic provenant de Cisco Webex. Si vous tentez de faire des recherches de connexion TCP, vous n'observerez aucune tentative de connexion pour Dst-port=5062 ou de processus subséquents de prise de contact mutuelle de MTLs ou d'invitation SIP provenant de Cisco Webex. Puisque la journalisation de diagnostic d'Expressway-E n'est d'aucun secours dans cette situation, vous disposez de quelques méthodes possibles pour la vérification :

1. Obtenez une saisie de paquets de l'interface externe du pare-feu
2. Tirez parti d'une fonctionnalité de vérification de port
3. Utilisez l'outil de test de connectivité d'Hybrid

Puisque l'outil de test de connectivité d'Hybrid est intégré au Cisco Webex Control Hub et simule l'environnement de Cisco Webex dans ses tentatives de connexion à l'Expressway sur les lieux, parmi les solutions offertes, c'est la méthode de vérification idéale. Pour mettre à l'essai la connectivité TCP dans l'organisation :

1. Ouvrez une session dans le Cisco Webex Control Hub
2. Sélectionnez les Services
3. Sélectionnez le lien conduisant aux paramètres (Settings) dans la carte Call card d'Hybrid.
4. Dans la section Call Service Connect, vérifiez que la valeur saisie dans le champ SIP Destination est correcte
5. Cliquez sur Test, comme l'indique l'image.

SIP Destination ⓘ



The screenshot shows a configuration field for 'SIP Destination' with the value '64.102.241.236:5062'. The field is highlighted in red, indicating an error. To the right of the field are two buttons: 'Test' (grey) and 'Save' (blue). Below the field, there is a red error message: 'Your SIP Destination is not configured correctly. View test results'.

6. Puisque l'essai a échoué, vous pouvez cliquer sur le lien d'affichage des résultats de test (**View test results**) pour consulter les détails, comme l'indique l'image.

Verify SIP Destination



IP address lookup

IP

64.102.241.236

Test for 64.102.241.236:5062		
Tests	Result	Details
Connecting to IP	Successful	
Socket test	Failed	TCP Connection failure: Check network connectivity, connection speed, and/or firewall configuration.
SSL Handshake	Not performed	
Ping	Not performed	

Comme l'illustre l'image ci-dessus, vous pouvez voir que le test de l'interface de connexion a échoué lors de la tentative de connexion au 64.102.241.236:5062. Grâce à ces données, en plus des journaux de diagnostic et pcaps Expressway qui n'affichent pas de tentatives de connexion, vous avez désormais assez de données probantes pour examiner la configuration du pare-feu ACL/NAT/routage.

Solution

Étant donné que ce problème en particulier n'est pas causé par l'environnement de Cisco Webex ou par l'équipement de collaboration sur les lieux, vous devez axer vos efforts sur la configuration du pare-feu. Puisque vous ne pouvez pas nécessairement prévoir le type de pare-feu avec lequel vous serez en contact, vous devrez vous fier à quelqu'un qui connaît le périphérique. Il est possible que le problème soit lié à une erreur de configuration de pare-feu ACL, de NAT ou de routage.

Problème 3. Échec du socket : Expressway-E n'est pas à l'écoute sur le port 5062

Il arrive souvent que ce problème en particulier ne soit pas correctement diagnostiqué. Souvent, il est supposé que le pare-feu est la cause du blocage du trafic sur le port 5062. Pour résoudre ce problème en particulier, vous pouvez utiliser les techniques décrites dans la mise en situation « Le port 5062 est bloqué à l'entrée d'Expressway » ci-dessus. Vous constaterez que l'outil de test de connectivité Hybrid échouera, comme tout autre outil pour vérifier la connectivité de port. Selon une première hypothèse, c'est le pare-feu qui bloquerait le trafic. La plupart des gens vérifieraient de nouveau la journalisation de diagnostic de l'Expressway-E pour déterminer s'ils peuvent repérer la connexion TCP qui tente de s'établir. De façon générale, ils chercheront à repérer une ligne de journal comme celle qui se trouve dans l'image.

```
2017-09-19T14:01:46.462-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 18:01:46,461"  
Module="network.tcp" Level="DEBUG": Src-ip="146.20.193.73" Src-port="40342" Dst-ip="172.16.2.2"  
Dst-port="5062" Detail="TCP Connecting"
```

Dans un cas comme celui-ci, l'entrée de journal ci-dessus n'apparaîtra pas. Par conséquent, plusieurs personnes établissent un diagnostic erroné en supposant que le problème vient du pare-feu.

Si une capture de paquets est incluse dans la journalisation de diagnostic, vous pouvez vérifier

que le pare-feu n'est pas la cause du problème. Voici un exemple de capture de paquets provenant du scénario dans lequel l'Expressway-E n'était pas à l'écoute sur le port 5062. Cette capture est filtrée avec le filtre `tcp.port==5062`, comme le révèle l'image.

No.	Time	Source	Destination	Protocol	S Port	D Port	Length	Info
55	2017-09-19 14:56:46.625745	146.20.193.73	172.16.2.2	TCP	34351	5062	74	34351->5062 [SYN] Seq=0 Win=14600 Len=0 MSS=1384
56	2017-09-19 14:56:46.625789	172.16.2.2	146.20.193.73	TCP	5062	34351	54	5062->34351 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
57	2017-09-19 14:56:46.653157	146.20.193.73	172.16.2.2	TCP	35883	5062	74	35883->5062 [SYN] Seq=0 Win=14600 Len=0 MSS=1384
58	2017-09-19 14:56:46.653173	172.16.2.2	146.20.193.73	TCP	5062	35883	54	5062->35883 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Annotations in the image:
 - Filter: `tcp.port==5062`
 - Spark TCP SYN packet received (pointing to packet 55)
 - Immediate RST sent from the Expressway (pointing to packet 56)

Comme vous pouvez le voir dans la capture de paquets obtenue à partir de l'Expressway-E, le trafic sur le port TCP 5062 n'est pas bloqué par le pare-feu. Au contraire, il est en train d'arriver. Dans le paquet numéro 56, vous pouvez voir que l'Expressway-E envoie le RST tout de suite après l'arrivée du premier paquet SYN. Compte tenu de cette information, vous pouvez conclure que le problème se limite à l'Expressway-E recevant le paquet; vous devez résoudre le problème sous l'angle de l'Expressway-E. Compte tenu des données probantes, envisagez les raisons possibles pour lesquelles l'Expressway-E appliquerait un RST au paquet. Voici deux scénarios possibles susceptibles de s'attribuer à ce comportement :

1. Dans l'Expressway-E, certains paramètres de pare-feu pourraient bloquer le trafic.
2. L'Expressway-E n'est pas à l'écoute du trafic de TLS mutuel ou du trafic sur le port 5062.

Les fonctionnalités de pare-feu de l'Expressway-E se trouvent sous *System > Protection > Firewall rules > Configuration*. Lorsque cela a été vérifié dans cet environnement, il n'y avait pas de configuration de pare-feu.

Il y a plusieurs façons de vérifier si l'Expressway-E est à l'écoute du trafic de TLS mutuel sur le port 5062. Vous pouvez le faire sur l'Interface Web ou la CLI en tant que superutilisateur.

Des racines de l'Expressway, si vous émettez `netstat -an | grep ' : 5062'`, vous devriez obtenir une sortie similaire à celle que vous voyez ci-dessous.

```
~ # netstat -an | grep ' : 5062'
tcp        0      0 172.16.2.2:5062      0.0.0.0:*           LISTEN    <-- Outside
Interface
tcp        0      0 192.168.1.6:5062     0.0.0.0:*           LISTEN    <-- Inside Interface
tcp        0      0 127.0.0.1:5062      0.0.0.0:*           LISTEN
tcp        0      0 :::5062              :::*                 LISTEN
```

Cette information peut aussi être saisie sur l'interface web de l'Expressway-E. Voir les étapes ci-dessous pour recueillir ces renseignements

1. Ouvrez une session dans l'Expressway-E
2. Naviguez jusqu'à **Maintenance Tools > Port usage > Local inbound ports**
3. Faites une recherche selon le Type SIP ou le port IP (IP port 5062). (en surbrillance en rouge, comme l'illustre l'image)

Type	Description	Protocol	IP address	IP port	Transport	Actions
H.323	Registration UDP port	H.323	192.168.1.6	1719	UDP	View/Edit
H.323	Registration UDP port	H.323	172.16.2.2	1719	UDP	View/Edit
SIP	TCP port	SIP	192.168.1.6	5060	TCP	View/Edit
SIP	TCP port	SIP	172.16.2.2	5060	TCP	View/Edit
SIP	TLS port	SIP	192.168.1.6	5061	TCP	View/Edit
SIP	TLS port	SIP	172.16.2.2	5061	TCP	View/Edit
SIP	Mutual TLS port	SIP	192.168.1.6	5062	TCP	View/Edit
SIP	Mutual TLS port	SIP	172.16.2.2	5062	TCP	View/Edit

Maintenant que vous savez ce que vous devriez voir, vous pouvez faire une comparaison avec l'environnement actuel. Dans la perspective de la CLI, lorsque vous exécutez `netstat -an | grep ':5062'`, la sortie ressemble à ceci :

```
~ # netstat -an | grep ':5062'
tcp        0      0 127.0.0.1:5062          0.0.0.0:*                LISTEN
tcp        0      0 :::1:5062                :::*                      LISTEN
~ #
```

En outre, l'UU web ne montre pas le port de TLS mutuel sous les ports entrants locaux

Type	Description	Protocol	IP address	IP port	Transport
H.323	Call signaling port range	H.323	192.168.1.6	15000-19999	TCP
H.323	Call signaling port range	H.323	172.16.2.2	15000-19999	TCP
H.323	Registration UDP port	H.323	192.168.1.6	1719	UDP
H.323	Registration UDP port	H.323	172.16.2.2	1719	UDP
SIP	TCP port	SIP	192.168.1.6	5060	TCP
SIP	TCP port	SIP	172.16.2.2	5060	TCP
SIP	TLS port	SIP	192.168.1.6	5061	TCP
SIP	TLS port	SIP	172.16.2.2	5061	TCP

Compte tenu de ces données, vous pouvez conclure que l'Expressway-E n'est pas à l'écoute du trafic de TLS mutuel.

Solution

Afin de résoudre ce problème, vous devez veiller à ce que le mode de TLS mutuel (Mutual TLS mode) soit activé et à ce que le port de TLS mutuel () soit réglé à 5062 sur l'Expressway-E :

1. Ouvrez une session dans l'Expressway-E
2. Naviguez jusqu'à **Configuration > Protocoles > SIP**
3. Vérifiez que le mode de prise de contact mutuelle de TLS (Mutual TLS mode) est activé (On)
4. Vérifiez que le port de prise de contact mutuelle de TLS (Mutual TLS port) est établi à **5062**
5. Cliquez sur **Save (enregistrer)**, comme l'indique l'image.

SIP

Configuration

SIP mode	On ▼ ⓘ
UDP mode	Off ▼ ⓘ
UDP port	★ 5060 ⓘ
TCP mode	On ▼ ⓘ
TCP port	★ 5060 ⓘ
TLS mode	On ▼ ⓘ
TLS port	★ 5061 ⓘ
Mutual TLS mode	On ▼ ⓘ
Mutual TLS port	★ 5062 ⓘ

Problème 4. Expressway-E ou C ne prend pas en charge les en-têtes de route SIP préchargés

Dans le contexte d'Hybrid Call Service Connect, l'appel de routage s'effectue en fonction **l'en-tête de routage**. L'en-tête de routage s'établit en fonction de l'information que fournit la partie Call Service Aware (connecteur Expressway) de la solution à Cisco Webex. L'hôte de connecteur Expressway interroge Unified CM pour les utilisateurs qui sont activés pour le service d'appel et extrait **l'URI de l'annuaire et le FQDN de groupe de leur grappe d'accueil Unified CM**. Voici des exemples mettant en vedette Alice et Bob :

URI de l'annuaire	En-tête de routage de la destination
bob@example.com	emea-cucm.example.com
alice@example.com	us-cucm.example.com

Si Alice ou Bob passe un appel, l'appel est acheminé vers l'Unified CM sur le site. Cela permet de relier l'appel au Cisco WebexRD avant de l'acheminer à l'utilisateur appelé.

Si Alice ont été appeler Bob, l' appel serait acheminer vers *Alice de Unified CM à la Maison Cluster FQDN (é.-cucm.example.com)*. Si vous analysez l'invitation (SIP INVITE) entrante que Cisco Webex envoie à l'Expressway-E, vous trouverez l'information suivante dans l'en-tête SIP.

Demande de création de lapos; URI sip :	bob@example.com
En-tête de routage	sip:us-cucm.example.com;lr

Du point de vue d'Expressway, les règles de recherche sont configurées pour acheminer l'appel non pas par l'URI de la demande, mais plutôt par **l'en-tête de route (us-cucm.example.com)** — dans ce cas, le cluster d'accueil Unified CM d'Alice.

Maintenant que les bases sont jetées, vous pouvez comprendre les situations de dépannage dans lesquelles l'Expressways fait l'objet d'une mauvaise configuration, qui entraîne le mauvais déroulement de la séquence logique décrite ci-dessus. Un peu comme on le constate pour presque tous les autres échecs de configuration d'Hybrid Call Service Connect, le symptôme est le suivant : *le téléphone sur les lieux ne sonne pas*.

Avant d'analyser les journaux de diagnostic sur l'Expressway, songez aux façons de cerner cet appel :

1. L'URI de demande de SIP sera l'**URI de l'annuaire de la partie appelée**.
2. Le champ SIP FROM sera formaté avec l'**appelant** indiqué comme « **Prénom** »
<sip:WebexDisplayName@subdomain.call.ciscospark.com>

Compte tenu de cette information, vous pouvez faire une recherche dans les journaux de diagnostic en fonction des paramètres suivants : **URI de l'Annuaire de la partie appelée, prénom et nom de la personne qui appelle ou adresse de SIP de Cisco Webex de la personne qui appelle**. Si vous n'avez aucune de ces informations, vous pouvez effectuer une recherche sur "INVITE SIP :" qui localise tous les appels SIP exécutés sur l'Expressway. Une fois que vous avez trouvé l'invitation de SIP de l'appel entrant, vous pouvez repérer et copier l'identifiant de l'appel SIP. Une fois que vous avez cette valeur, vous pouvez simplement faire une recherche dans les journaux de diagnostic en fonction de l'identifiant de l'appel pour voir tous les messages s'attachant à ce segment d'appel.

Une autre façon de contribuer à isoler le problème de routage consiste à déterminer quelle distance l'appel parvient à franchir dans l'entreprise. Vous pouvez essayer d'effectuer des recherches ayant pour objet les renseignements précisés ci-dessus sur l'Expressway-C pour voir

si l'appel a été acheminé jusque-là. Si c'est le cas, c'est probablement là que vous voudrez lancer votre étude.

Dans ce scénario, vous pouvez voir que l'Expressway-C a reçu l'invitation (INVITE) de l'Expressway-E.

```
2017-09-19T14:16:15.836-04:00 rtp12-tpdmz-118-VCSC tvcs: UTCTime="2017-09-19 18:16:15,830"
Module="network.sip" Level="DEBUG": Action="Received" Local-ip="192.168.1.5" Local-port="26847"
Src-ip="192.168.1.6" Src-port="7003" Msg-Hash="11449260850208794722"
SIPMSG:
|INVITE sip:jorobb@rtp.ciscotac.net SIP/2.0
Via: SIP/2.0/TLS 192.168.1.6:7003;egress-
zone=HybridCallServiceTraversal;branch=z9hG4bKc81c6c4dddef7ed6be5bdce9868fb019913;proxy-call-
id=a82052ef-6fd7-4506-8173-e73af6655b5d;rport
Via: SIP/2.0/TLS 192.168.1.6:5073;branch=z9hG4bKb0eba6d700dfdf761a8ad97fff3c240124;x-cisco-
local-service=nettle;received=192.168.1.6;rport=43119;ingress-zone=DefaultZone
Via: SIP/2.0/TLS 64.102.241.236:5061;egress-
zone=DefaultZone;branch=z9hG4bK6fe399bae58fb0d70c9d69b8e37e13e5912.4248943487bff4af6f649b586c769
6bb;proxy-call-id=f2d15853-c81f-462f-b3e5-c08124f344a3;received=172.16.2.2;rport=25016
Via: SIP/2.0/TLS
192.168.5.66:5062;branch=z9hG4bK0f455ca79cf1b0af5637333aa5286436;received=146.20.193.45;rport=35
464;ingress-zone=HybridCallServicesDNS
Via: SIP/2.0/TLS 127.0.0.1:5070;branch=z9hG4bK-383039-
8f0d64025c04d23b6d5e1d5142db46ec;rport=52706
Call-ID: 9062bca7eca2afe71b4a225048ed5101@127.0.0.1
CSeq: 1 INVITE
Contact: <sip:192.168.1.6:5073;transport=tls>;call-type=squared
From: "pstoiano test"
```

```
;tag=872524918
To: <sip:jorobb@rtp.ciscotac.net>
Max-Forwards: 15
Route:
```

```
Record-Route: <sip:proxy-call-id=a82052ef-6fd7-4506-8173-
e73af6655b5d@192.168.1.6:7003;transport=tls;lr>
Record-Route: <sip:proxy-call-id=a82052ef-6fd7-4506-8173-
e73af6655b5d@192.168.1.6:5061;transport=tls;lr>
```

La partie importante : l'en-tête de routage (FQDN de grappe) demeure intacte. Toutefois, il n'y a aucune logique de recherche s'exécutant en fonction de l'en-tête de routage (FQDN de grappe) **cucm.rtp.ciscotac.net**. Vous constatez plutôt que le message est rejeté immédiatement et fait l'objet d'un message d'erreur **404 Not Found**.

```
2017-09-19T14:16:15.836-04:00 rtp12-tpdmz-118-VCSC tvcs: Event="Call Attempted" Service="SIP"
Src-ip="192.168.1.6" Src-port="7003" Src-alias-type="SIP" Src-alias="sip:pstoiano-
test@dmzlab.call.ciscopark.com" Dst-alias-type="SIP" Dst-alias="sip:jorobb@rtp.ciscotac.net"
Call-serial-number="a3e44231-f62a-4e95-a70e-253701a89515" Tag="73c276e2-3917-4a0c-9fc5-
ddde83b49fd0" Protocol="TLS" Auth="NO" Level="1" UTCTime="2017-09-19 18:16:15,832"
2017-09-19T14:16:15.836-04:00 rtp12-tpdmz-118-VCSC tvcs: Event="Search Attempted" Service="SIP"
Src-alias-type="SIP" Src-alias="pstoiano-test@dmzlab.call.ciscopark.com" Dst-alias-type="SIP"
Dst-alias="sip:jorobb@rtp.ciscotac.net" Call-serial-number="a3e44231-f62a-4e95-a70e-
253701a89515" Tag="73c276e2-3917-4a0c-9fc5-ddde83b49fd0" Detail="searchtype:INVITE" Level="1"
```

UTCtime="2017-09-19 18:16:15,834"
2017-09-19T14:16:15.836-04:00 rtp12-tpdmz-118-VCSC tvcs: Event="Search Completed" Reason="Not Found" Service="SIP" Src-alias-type="SIP" Src-alias="pstojoano-test@dmzlab.call.ciscospark.com" Dst-alias-type="SIP" Dst-alias="sip:jorobb@rtp.ciscotac.net" Call-serial-number="a3e44231-f62a-4e95-a70e-253701a89515" Tag="73c276e2-3917-4a0c-9fc5-ddde83b49fd0" Detail="found:false, searchtype:INVITE, Info:Policy Response" Level="1" UTCtime="2017-09-19 18:16:15,835"
2017-09-19T14:16:15.836-04:00 rtp12-tpdmz-118-VCSC tvcs: Event="Call Rejected" Service="SIP" Src-ip="192.168.1.6" Src-port="7003" Src-alias-type="SIP" Src-alias="sip:pstojoano-test@dmzlab.call.ciscospark.com" Dst-alias-type="SIP" Dst-alias="sip:jorobb@rtp.ciscotac.net" Call-serial-number="a3e44231-f62a-4e95-a70e-253701a89515" Tag="73c276e2-3917-4a0c-9fc5-ddde83b49fd0" Detail="Not Found" Protocol="TLS" Response-code="404" Level="1" UTCtime="2017-09-19 18:16:15,835"
2017-09-19T14:16:15.836-04:00 rtp12-tpdmz-118-VCSC tvcs: UTCtime="2017-09-19 18:16:15,830" Module="network.sip" Level="INFO": Action="Received" Local-ip="192.168.1.5" Local-port="26847" Src-ip="192.168.1.6" Src-port="7003" Detail="Receive Request Method=INVITE, CSeq=1, Request-URI=sip:jorobb@rtp.ciscotac.net, Call-ID=9062bca7eca2afe71b4a225048ed5101@127.0.0.1, From-Tag=872524918, To-Tag=, Msg-Hash=11449260850208794722, Local-SessionID=daf7c278732bb5a557fb57925dffcbf7, Remote-SessionID=00000000000000000000000000000000" 2017-09-19T14:16:15.836-04:00 rtp12-tpdmz-118-VCSC tvcs: UTCtime="2017-09-19 18:16:15,836" Module="network.sip" Level="INFO": Action="Sent" Local-ip="192.168.1.5" Local-port="26847" Dst-ip="192.168.1.6" Dst-port="7003" Detail="Sending Response Code=404, Method=INVITE, CSeq=1, To=sip:jorobb@rtp.ciscotac.net, Call-ID=9062bca7eca2afe71b4a225048ed5101@127.0.0.1, From-Tag=872524918, To-Tag=96b9a0eaf669a590, Msg-Hash=254718822158415175, Local-SessionID=00000000000000000000000000000000, Remote-SessionID=daf7c278732bb5a557fb57925dffcbf7"
2017-09-19T14:16:15.836-04:00 rtp12-tpdmz-118-VCSC tvcs: UTCtime="2017-09-19 18:16:15,836" Module="network.sip" Level="DEBUG": Action="Sent" Local-ip="192.168.1.5" Local-port="26847" Dst-ip="192.168.1.6" Dst-port="7003" Msg-Hash="254718822158415175"
SIPMSG:
|SIP/2.0 404 Not Found
Via: SIP/2.0/TLS 192.168.1.6:7003;egress-zone=HybridCallServiceTraversal;branch=z9hG4bKc81c6c4dddef7ed6be5bdce9868fb019913;proxy-call-id=a82052ef-6fd7-4506-8173-e73af6655b5d;received=192.168.1.6;rport=7003;ingress-zone=HybridCallServiceTraversal
Via: SIP/2.0/TLS 192.168.1.6:5073;branch=z9hG4bKb0eba6d700dfd761a8ad97fff3c240124;x-cisco-local-service=nettle;received=192.168.1.6;rport=43119;ingress-zone=DefaultZone
Via: SIP/2.0/TLS 64.102.241.236:5061;egress-zone=DefaultZone;branch=z9hG4bK6fe399bae58fb0d70c9d69b8e37e13e5912.4248943487bff4af6f649b586c7696bb;proxy-call-id=f2d15853-c81f-462f-b3e5-c08124f344a3;received=172.16.2.2;rport=25016
Via: SIP/2.0/TLS 192.168.5.66:5062;branch=z9hG4bK0f455ca79cf1b0af5637333aa5286436;received=146.20.193.45;rport=35464;ingress-zone=HybridCallServicesDNS
Via: SIP/2.0/TLS 127.0.0.1:5070;branch=z9hG4bK-383039-8f0d64025c04d23b6d5e1d5142db46ec;rport=52706
Call-ID: 9062bca7eca2afe71b4a225048ed5101@127.0.0.1
CSeq: 1 INVITE
From: "pstojoano test"

;tag=872524918
To: <sip:jorobb@rtp.ciscotac.net>;tag=96b9a0eaf669a590
Server: TANDBERG/4135 (X8.10.2)
Warning: 399 192.168.1.5:5061 "Policy Response"
Session-ID: 00000000000000000000000000000000;remote=daf7c278732bb5a557fb57925dffcbf7
Content-Length: 0

Si l'on compare avec un scénario de fonctionnement, dans un tel scénario, la logique de recherche s'exécuterait selon l'en-tête de routage (FQDN de grappe)


```
2017-09-22T13:56:02.215-04:00 rtp12-tpdmz-118-VCSC tvcs: Event="Search Attempted" Service="SIP"
Src-alias-type="SIP" Src-alias="pstojano-test@dmzlab.call.ciscopark.com" Dst-alias-type="SIP"
Dst-alias="sip:jorobb@rtp.ciscotac.net" Call-serial-number="17aa8dc7-422c-42ef-bdd9-
b9750fbd0edf" Tag="8bd936da-f2ab-4412-96df-d64558f7597b" Detail="searchtype:INVITE" Level="1"
UTCTime="2017-09-22 17:56:02,215"
2017-09-22T13:56:02.218-04:00 rtp12-tpdmz-118-VCSC tvcs: UTCTime="2017-09-22 17:56:02,217"
Module="network.cpl" Level="DEBUG": Remote-ip="192.168.1.6" Remote-port="7003" Detail="CPL:
<routed> "
2017-09-22T13:56:02.218-04:00 rtp12-tpdmz-118-VCSC tvcs: UTCTime="2017-09-22 17:56:02,218"
Module="network.cpl" Level="DEBUG": Remote-ip="192.168.1.6" Remote-port="7003" Detail="CPL:
<location clear="yes" url="sip:cucm.rtp.ciscotac.net;lr" diversion="" dest-url-for-
message="sip:jorobb@rtp.ciscotac.net" sip-route-set="" dest-service=""> added
sip:cucm.rtp.ciscotac.net;lr to location set "
2017-09-22T13:56:02.218-04:00 rtp12-tpdmz-118-VCSC tvcs: UTCTime="2017-09-22 17:56:02,218"
Module="network.cpl" Level="DEBUG": Remote-ip="192.168.1.6" Remote-port="7003" Detail="CPL:
<proxy stop-on-busy="no" timeout="0"/> "
2017-09-22T13:56:02.218-04:00 rtp12-tpdmz-118-VCSC tvcs: UTCTime="2017-09-22 17:56:02,218"
Module="network.search" Level="DEBUG": Detail="Search rule 'Inbound MS to CMS' did not match
destination alias 'cucm.rtp.ciscotac.net;lr'"
2017-09-22T13:56:02.218-04:00 rtp12-tpdmz-118-VCSC tvcs: UTCTime="2017-09-22 17:56:02,218"
Module="network.search" Level="DEBUG": Detail="Search rule 'multiway' did not match destination
alias 'cucm.rtp.ciscotac.net;lr'"
2017-09-22T13:56:02.218-04:00 rtp12-tpdmz-118-VCSC tvcs: UTCTime="2017-09-22 17:56:02,218"
Module="network.search" Level="DEBUG": Detail="Search rule 'WebEx Search Rule' did not match
destination alias 'cucm.rtp.ciscotac.net;lr'"
2017-09-22T13:56:02.218-04:00 rtp12-tpdmz-118-VCSC tvcs: UTCTime="2017-09-22 17:56:02,218"
Module="network.search" Level="DEBUG": Detail="Search rule 'ISDN Inbound' ignored due to source
filtering"
2017-09-22T13:56:02.218-04:00 rtp12-tpdmz-118-VCSC tvcs: UTCTime="2017-09-22 17:56:02,218"
Module="network.search" Level="DEBUG": Detail="Search rule 'recalls into CMS' did not match
destination alias 'cucm.rtp.ciscotac.net;lr'"
2017-09-22T13:56:02.218-04:00 rtp12-tpdmz-118-VCSC tvcs: UTCTime="2017-09-22 17:56:02,218"
Module="network.search" Level="DEBUG": Detail="Search rule 'CBtcp-rtp12-tpdmz-118-ucmpub' did
not match destination alias 'cucm.rtp.ciscotac.net;lr'"
2017-09-22T13:56:02.218-04:00 rtp12-tpdmz-118-VCSC tvcs: UTCTime="2017-09-22 17:56:02,218"
Module="network.search" Level="DEBUG": Detail="Search rule 'Conference Factory' did not match
destination alias 'cucm.rtp.ciscotac.net;lr'"
2017-09-22T13:56:02.218-04:00 rtp12-tpdmz-118-VCSC tvcs: UTCTime="2017-09-22 17:56:02,219"
Module="network.search" Level="DEBUG": Detail="Search rule 'Inbound B2B Calling' did not match
destination alias 'cucm.rtp.ciscotac.net;lr'"
2017-09-22T13:56:02.218-04:00 rtp12-tpdmz-118-VCSC tvcs: UTCTime="2017-09-22 17:56:02,219"
Module="network.search" Level="DEBUG": Detail="Search rule 'Calls to Cisco Webex' did not match
destination alias 'cucm.rtp.ciscotac.net;lr'"
2017-09-22T13:56:02.218-04:00 rtp12-tpdmz-118-VCSC tvcs: UTCTime="2017-09-22 17:56:02,219"
Module="network.search" Level="DEBUG": Detail="Considering search rule 'as is local' towards
target 'LocalZone' at priority '1' with alias 'cucm.rtp.ciscotac.net;lr'"
2017-09-22T13:56:02.219-04:00 rtp12-tpdmz-118-VCSC tvcs: UTCTime="2017-09-22 17:56:02,219"
Module="network.search" Level="DEBUG": Detail="Considering search rule 'Hybrid Call Service
Inbound Routing' towards target 'CUCM11' at priority '2' with alias 'cucm.rtp.ciscotac.net;lr'"
```

On peut ensuite voir que l'Expressway-C transmet correctement l'appel vers Unified CM (192.168.1.21).

```
2017-09-22T13:56:02.232-04:00 rtp12-tpdmz-118-VCSC tvcs: UTCTime="2017-09-22 17:56:02,232"
Module="network.sip" Level="DEBUG": Action="Sent" Local-ip="192.168.1.5" Local-port="25606" Dst-
ip="192.168.1.21" Dst-port="5065" Msg-Hash="866788495063340574"
SIPMSG:
|INVITE sip:jorobb@rtp.ciscotac.net SIP/2.0
Via: SIP/2.0/TCP 192.168.1.5:5060;egress-
zone=CUCM11;branch=z9hg4bK251d6daf044e635607cc13d244b9ea45138220.69ccb8de20a0e853c1313782077f77b
5;proxy-call-id=17aa8dc7-422c-42ef-bdd9-b9750fbd0edf;rport
Via: SIP/2.0/TLS 192.168.1.6:7003;egress-
```

zone=HybridCallServiceTraversal;branch=z9hG4bKba323da436b2bc288200d56d11f02d4d272;proxy-call-id=32c76cef-e73c-4911-98d0-e2d2bb6fec77;received=192.168.1.6;rport=7003;**ingress-**

zone=HybridCallServiceTraversal

Via: SIP/2.0/TLS 192.168.1.6:5073;branch=z9hG4bK06cde3f662d53a210b5b4b11b85500c19;x-cisco-local-service=nettle;received=192.168.1.6;rport=42533;ingress-zone=DefaultZone

Via: SIP/2.0/TLS 64.102.241.236:5061;egress-

zone=DefaultZone;branch=z9hG4bK297799f31d0785ff7449e1d7dbe3595b271.2ed90cbcd5b79c6cffad9ecd84cc8337;proxy-call-id=3be87d96-d2e6-4489-b936-8f9cb5ccaa5f;received=172.16.2.2;rport=25005

Via: SIP/2.0/TLS

192.168.4.146:5062;branch=z9hG4bK043ca6360f253c6abed9b23fbfeff9819;received=148.62.40.64;rport=36149;ingress-zone=HybridCallServicesDNS

Via: SIP/2.0/TLS 127.0.0.1:5070;branch=z9hG4bK-353038-

8c648a16c2c5d7b85fa5c759d59aa190;rport=47732

Call-ID: daa1a6fa546ce76591fc464f0a50ee32@127.0.0.1

CSeq: 1 INVITE

Contact: <sip:192.168.1.6:5073;transport=tls>;call-type=squared

From: "pstoiano test" <sip:pstoiano-test@dmzlab.call.ciscospark.com>;tag=567490631

To: <sip:jorobb@rtp.ciscotac.net>

Max-Forwards: 14

Route:

Record-Route: <sip:proxy-call-id=17aa8dc7-422c-42ef-bdd9-b9750fbd0edf@192.168.1.5:5060;transport=tcp;lr>

Record-Route: <sip:proxy-call-id=17aa8dc7-422c-42ef-bdd9-b9750fbd0edf@192.168.1.5:5061;transport=tls;lr>

Record-Route: <sip:proxy-call-id=32c76cef-e73c-4911-98d0-e2d2bb6fec77@192.168.1.6:7003;transport=tls;lr>

Record-Route: <sip:proxy-call-id=32c76cef-e73c-4911-98d0-e2d2bb6fec77@192.168.1.6:5061;transport=tls;lr>

Allow: INVITE,ACK,BYE,CANCEL,INFO,OPTIONS,REFER,SUBSCRIBE,NOTIFY

User-Agent: TANDBERG/4352 (X8.10.2-b2bua-1.0)

À la suite de cette analyse de la journalisation de diagnostic, qui a permis de constater que le problème se limite à l'Expressway-C et plus particulièrement, qu'il s'attribue à une erreur précise (404 Not Found), vous pouvez axer vos efforts sur ce qui cause ce type de comportement. Voici certains aspects à envisager :

1. Les appels sont déplacés entre les zones de l'Expressway au moyen de règles de recherche.
2. L'Expressways fait appel à une logique préétablie de prise en charge du routage SIP (Preloaded SIP routes support). Cela permet de traiter les demandes d'invitation de SIP qui contiennent des en-têtes de routage. Il est possible d'activer ou de désactiver cette valeur dans les zones (serveur de traverse, client de traverse, voisin) sur l'Expressway-C et l'Expressway-E.

Vous pouvez désormais utiliser xConfiguration pour afficher la configuration du serveur de traverse Expressway-E et des zones client de l'Expressway-C, surtout lorsque ces configurations sont destinées à Hybrid Call Service Connect. Outre la configuration de la zone, vous pouvez analyser les règles de recherche qui sont configurées pour transmettre cet appel d'une zone à l'autre. Vous savez également que l'Expressway-E a communiqué l'appel vers l'Expressway-C. Ainsi, la configuration de la zone du serveur de traverse est probablement bien effectuée.

Approfondissons cette question. Vous verrez ci-dessous que xConfig indique que cette zone s'appelle **Hybrid Call ServiceTraversal** (traverse d'Hybrid Call Service). Il s'agit d'un type de zone **TraversalServer**. Ce type communique avec l'Expressway-C sur le port TCP de SIP **7003**.

Pour le l'Hybrid Call Service, l'élément central est que la prise en charge Preloaded SIP routes support doit être activée. Dans l'interface Web d'Expressway, cette valeur s'appelle **Preloaded SIP routes support**, tandis que xConfiguration l'affichera sous l'appellation **SIP PreloadedSipRoutes Accept**

Expressway-E

```
*c xConfiguration Zones Zone 7 Name: "Hybrid Call Service Traversal"
*c xConfiguration Zones Zone 7 TraversalServer Authentication Mode: "DoNotCheckCredentials"
*c xConfiguration Zones Zone 7 TraversalServer Authentication UserName: "hybridauth"
*c xConfiguration Zones Zone 7 TraversalServer Collaboration Edge: "Off"
*c xConfiguration Zones Zone 7 TraversalServer H323 H46019 Demultiplexing Mode: "Off"
*c xConfiguration Zones Zone 7 TraversalServer H323 Port: "6007"
*c xConfiguration Zones Zone 7 TraversalServer H323 Protocol: "Assent"
*c xConfiguration Zones Zone 7 TraversalServer Registrations: "Allow"
*c xConfiguration Zones Zone 7 TraversalServer SIP Media AesGcm Support: "Off"
*c xConfiguration Zones Zone 7 TraversalServer SIP Media Encryption Mode: "Auto"
*c xConfiguration Zones Zone 7 TraversalServer SIP Media ICE Support: "Off"
*c xConfiguration Zones Zone 7 TraversalServer SIP Multistream Mode: "On"
*c xConfiguration Zones Zone 7 TraversalServer SIP ParameterPreservation Mode: "On"
*c xConfiguration Zones Zone 7 TraversalServer SIP Poison Mode: "Off"
*c xConfiguration Zones Zone 7 TraversalServer SIP Port: "7003"
*c xConfiguration Zones Zone 7 TraversalServer SIP PreloadedSipRoutes Accept: "On"
*c xConfiguration Zones Zone 7 TraversalServer SIP Protocol: "Assent"
*c xConfiguration Zones Zone 7 TraversalServer SIP TLS Verify Mode: "On"
*c xConfiguration Zones Zone 7 TraversalServer SIP TLS Verify Subject Name: "rtp12-tpdmz-118-
VCSC.rtp.ciscotac.net"
*c xConfiguration Zones Zone 7 TraversalServer SIP Transport: "TLS"
*c xConfiguration Zones Zone 7 TraversalServer TCPProbe KeepAliveInterval: "20"
*c xConfiguration Zones Zone 7 TraversalServer TCPProbe RetryCount: "5"
*c xConfiguration Zones Zone 7 TraversalServer TCPProbe RetryInterval: "2"
*c xConfiguration Zones Zone 7 TraversalServer UDPProbe KeepAliveInterval: "20"
*c xConfiguration Zones Zone 7 TraversalServer UDPProbe RetryCount: "5"
*c xConfiguration Zones Zone 7 TraversalServer UDPProbe RetryInterval: "2"
*c xConfiguration Zones Zone 7 Type: "TraversalServer"
```

Vous pouvez également déterminer que cette zone est reliée à une règle 3 de recherche (Webex Hybrid). Essentiellement, la règle de recherche communique un alias correspondant à « l'un ou l'autre », par l'entremise de la zone DNS. Celui-ci est ensuite transmis à la zone au-dessus, la traverse Hybrid Call Service. Comme l'on pouvait s'y attendre, la règle de recherche et la zone de serveur de traverse sont configurées correctement sur l'Expressway-E.

```
*c xConfiguration Zones Policy SearchRules Rule 3 Authentication: "No"
*c xConfiguration Zones Policy SearchRules Rule 3 Description: "Calls to VCS-C"
*c xConfiguration Zones Policy SearchRules Rule 3 Mode: "AnyAlias"
*c xConfiguration Zones Policy SearchRules Rule 3 Name: "Webex Hybrid"
*c xConfiguration Zones Policy SearchRules Rule 3 Pattern Behavior: "Strip"
*c xConfiguration Zones Policy SearchRules Rule 3 Pattern Replace:
*c xConfiguration Zones Policy SearchRules Rule 3 Pattern String:
*c xConfiguration Zones Policy SearchRules Rule 3 Pattern Type: "Prefix"
*c xConfiguration Zones Policy SearchRules Rule 3 Priority: "15"
*c xConfiguration Zones Policy SearchRules Rule 3 Progress: "Stop"
*c xConfiguration Zones Policy SearchRules Rule 3 Protocol: "SIP"
*c xConfiguration Zones Policy SearchRules Rule 3 SIPTrafficType: "Any"
*c xConfiguration Zones Policy SearchRules Rule 3 Source Mode: "Named"
*c xConfiguration Zones Policy SearchRules Rule 3 Source Name: "Hybrid Call Services DNS"
*c xConfiguration Zones Policy SearchRules Rule 3 State: "Enabled"
*c xConfiguration Zones Policy SearchRules Rule 3 SystemGenerated: "No"
*c xConfiguration Zones Policy SearchRules Rule 3 Target Name: "Hybrid Call Service Traversal"
*c xConfiguration Zones Policy SearchRules Rule 3 Target SIPVariant: "Any"
*c xConfiguration Zones Policy SearchRules Rule 3 Target Type: "Zone"
```

Si vous mettez l'accent sur xConfiguration de l'Expressway-c, vous pouvez commencer par examiner la zone client de traverse pour Webex Hybrid. Pour la trouver facilement, faites une recherche sur le numéro de port découvert grâce à xConfiguration sur l'Expressway-E (**Port de SIP : « 7003 »**). Cela vous permet de cerner rapidement la zone correcte dans xConfiguration.

Comme il en a été question auparavant, vous pouvez apprendre le nom de zone (Hybrid Call Service Traversal), le type (Traversal Client) et les autres aspects configurés pour la fonction SIP PreloadedSipRoutes Accept (Preloaded SIP routes support). Comme vous pouvez le voir dans xConfiguration, cette valeur est désactivée (« Off »). Selon le guide de déploiement pour Cisco Webex Hybrid Call Services, cette valeur doit être activée (« On »).

En outre, à la lecture de la définition de la fonction Preloaded SIP routes support, on constate qu'il est clairement indiqué que l'Expressway-C doit REFUSER un message si cette valeur est désactivée ET que l'invitation (INVITE) comprend un en-tête de routage : **« Preloaded SIP routes support doit être désactivé (« Off ») si vous souhaitez que la zone rejette les demandes d'invitation de SIP avec un en-tête. »**

Expressway-C

```
*c xConfiguration Zones Zone 6 Name: "Hybrid Call Service Traversal"
*c xConfiguration Zones Zone 6 TraversalClient Accept Delegated Credential Checks: "Off"
*c xConfiguration Zones Zone 6 TraversalClient Authentication Mode: "DoNotCheckCredentials"
*c xConfiguration Zones Zone 6 TraversalClient Authentication Password:
"{cipher}qeh8eq+fuVY1GHGgRLder/11YDd76O/6KrHGA7g8bJs="
*c xConfiguration Zones Zone 6 TraversalClient Authentication UserName: "hybridauth"
*c xConfiguration Zones Zone 6 TraversalClient Collaboration Edge: "Off"
*c xConfiguration Zones Zone 6 TraversalClient H323 Port: "1719"
*c xConfiguration Zones Zone 6 TraversalClient H323 Protocol: "Assent"
*c xConfiguration Zones Zone 6 TraversalClient Peer 1 Address: "amer-expressway01.ciscotac.net"
*c xConfiguration Zones Zone 6 TraversalClient Peer 2 Address:
*c xConfiguration Zones Zone 6 TraversalClient Peer 3 Address:
*c xConfiguration Zones Zone 6 TraversalClient Peer 4 Address:
*c xConfiguration Zones Zone 6 TraversalClient Peer 5 Address:
*c xConfiguration Zones Zone 6 TraversalClient Peer 6 Address:
*c xConfiguration Zones Zone 6 TraversalClient Registrations: "Allow"
*c xConfiguration Zones Zone 6 TraversalClient RetryInterval: "120"
*c xConfiguration Zones Zone 6 TraversalClient SIP Media AesGcm Support: "Off"
*c xConfiguration Zones Zone 6 TraversalClient SIP Media Encryption Mode: "Auto"
*c xConfiguration Zones Zone 6 TraversalClient SIP Media ICE Support: "Off"
*c xConfiguration Zones Zone 6 TraversalClient SIP Multistream Mode: "On"
*c xConfiguration Zones Zone 6 TraversalClient SIP ParameterPreservation Mode: "On"
*c xConfiguration Zones Zone 6 TraversalClient SIP Poison Mode: "Off"
*c xConfiguration Zones Zone 6 TraversalClient SIP Port: "7003"
*c xConfiguration Zones Zone 6 TraversalClient SIP PreloadedSipRoutes Accept: "Off"
*c xConfiguration Zones Zone 6 TraversalClient SIP Protocol: "Assent"
*c xConfiguration Zones Zone 6 TraversalClient SIP TLS Verify Mode: "On"
*c xConfiguration Zones Zone 6 TraversalClient SIP TURN Server Address:
*c xConfiguration Zones Zone 6 TraversalClient SIP TURN Server Port:
*c xConfiguration Zones Zone 6 TraversalClient SIP Transport: "TLS"
*c xConfiguration Zones Zone 6 Type: "TraversalClient"
```

À ce stade, vous avez établi que le problème se limite à une erreur de configuration de la zone client de traverse d'Expressway-C. Vous devez activer la prise en charge Preloaded SIP routes support (« On »)

Solution

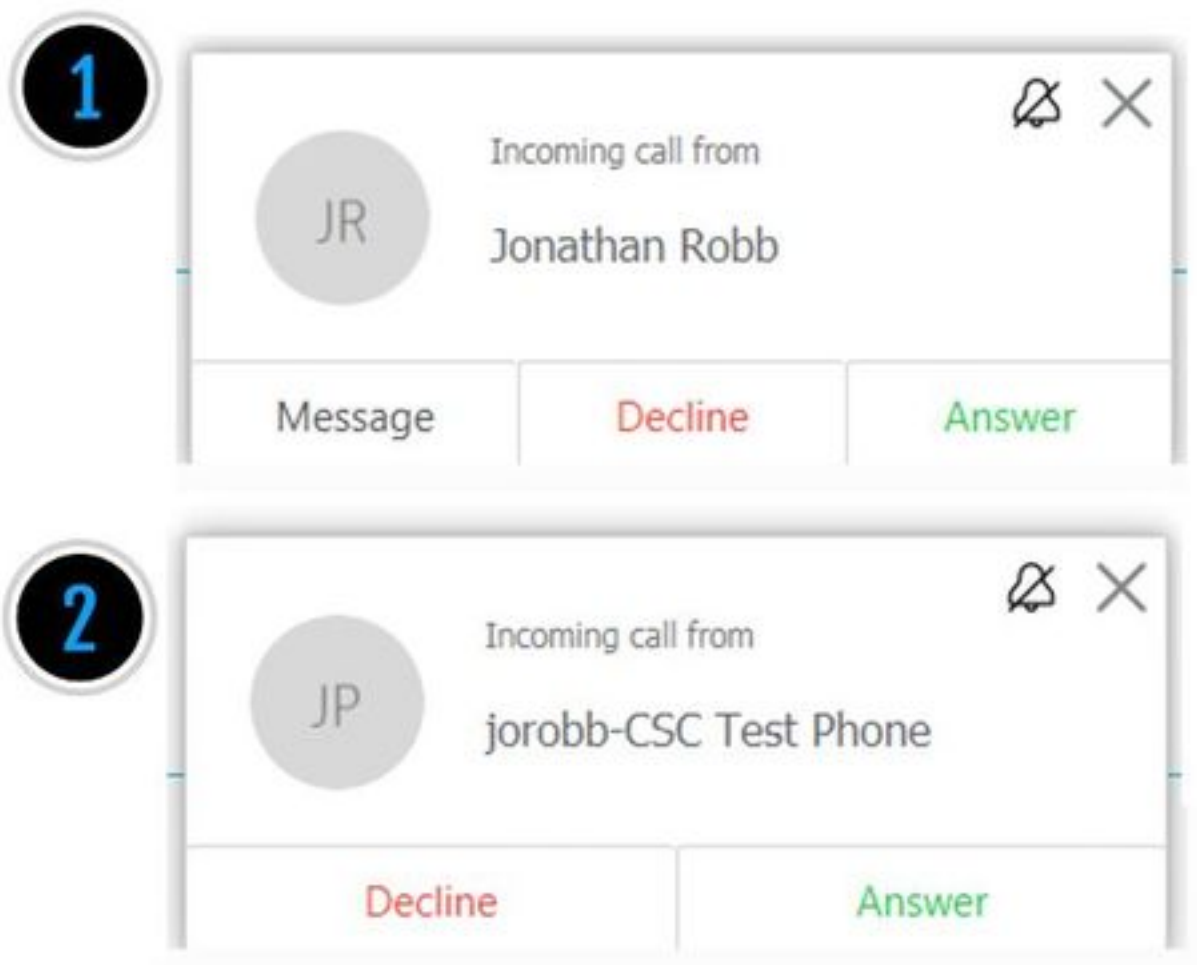
Pour configurer correctement la prise en charge Preloaded SIP routes support :

1. Ouvrez une session dans l'Expressway-E
2. Naviguez jusqu'à **Configuration > Zones > Zones**
3. Sélectionnez la zone de client de traverse d'Hybrid Call Service (le nom variera selon le client)
4. Définir la prise en charge **Preloaded SIP routes support** pour qu'elle soit activée (« On »)
5. Sélectionnez **Save (enregistrer)**

Note: Tandis que ce scénario a mis en évidence une défaillance sur l'Expressway-C, les mêmes erreurs de journalisation de diagnostic pourraient s'observer sur l'Expressway-E si la prise en charge **Preloaded SIP routes support** a été désactivée dans la zone du serveur de traverse **Webex Hybrid Call**. Si c'était le cas, l'appel n'aurait jamais atteint l'Expressway-C et c'est l'Expressway-E qui aurait été responsable de rejeter l'appel et d'envoyer l'erreur 404 Not Found.

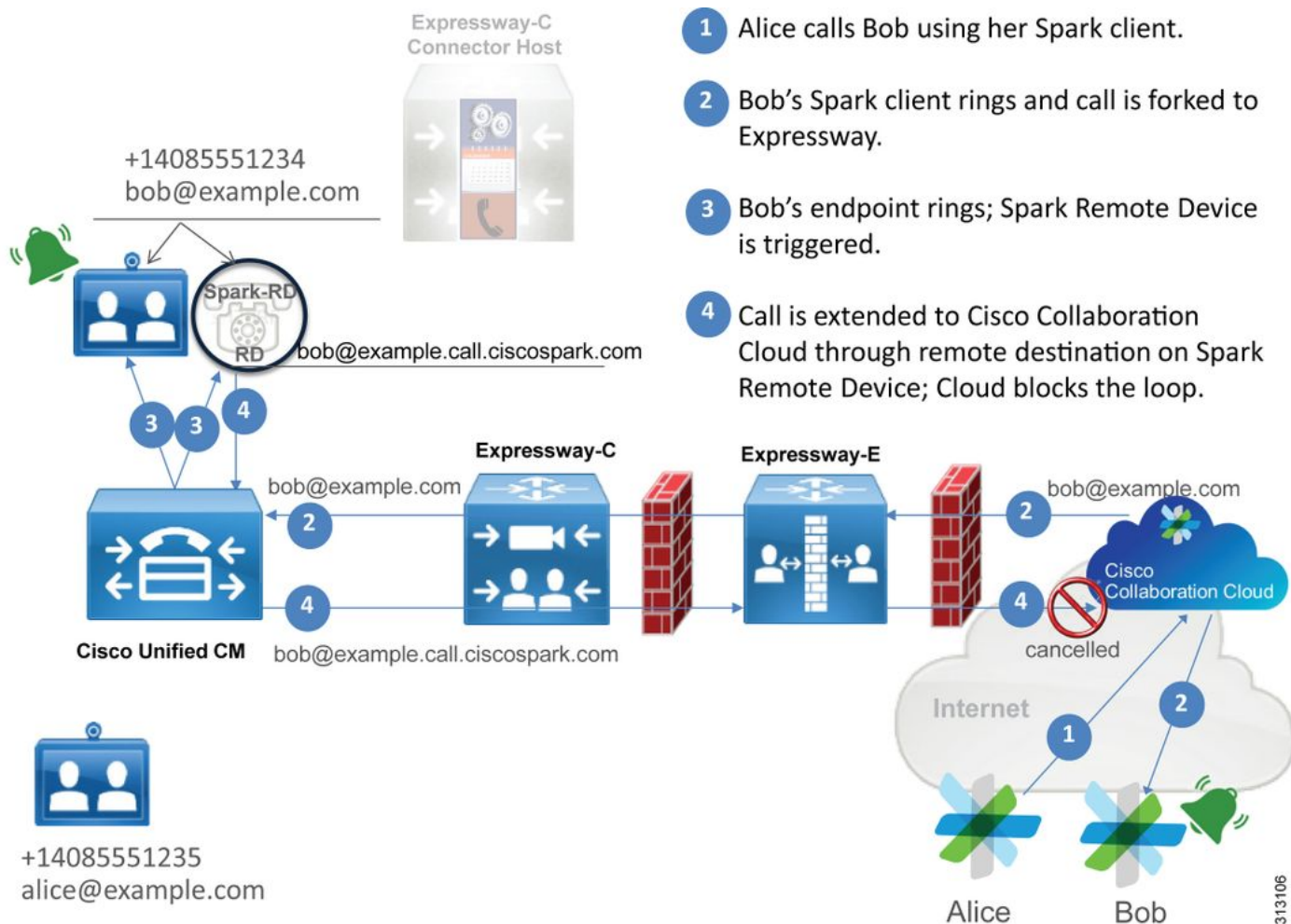
Problème 5. L'application Cisco Webex reçoit deux notifications d'appel (toasts)

Ce problème en particulier est le seul scénario d'appels entrants qui ne conduit pas à une interruption d'appel. Lorsque ce problème survient, la personne recevant l'appel (l'appelé) reçoit deux notifications (ou invites) dans l'application Cisco Webex de la part de la personne qui a fait l'appel (la partie appelante). La première notification provient de Cisco Webex et la deuxième vient de l'infrastructure sur place. Ci-dessous, vous trouverez des échantillons des notifications reçues, comme l'illustre l'image.



La première notification (invite) vient de la personne qui a lancé l'appel (la partie appelante) du côté de Cisco Webex. Dans ce cas-ci, l'ID de l'appelant est le nom d'affichage de l'utilisateur qui a

lancé l'appel. La deuxième notification (invite) provient de la CTI sur place ou de Cisco Webex RD qui est affecté à l'utilisateur qui passe l'appel. Au départ, ce comportement semble étrange. Cependant, si vous passez en revue le diagramme des appels entrants (dans le guide de conception de Cisco Webex Hybrid), le comportement semble plus logique, comme le révèle l'image.



L'illustration montre qu'Alice appelle Bob au moyen de son application Cisco Webex. L'appel est transmis vers le site sur place. Cet appel devrait correspondre à l'URI de l'annuaire s'attribuant au téléphone de Bob. Le problème vient de ce que dans cette conception, l'URI de l'annuaire s'attache aussi au CTI-RD ou au Cisco Webex RD de Bob. Par conséquent, lorsque l'appel est communiqué à CTI-RD ou à Cisco Webex RD, l'appel est renvoyé vers Cisco Webex, car la configuration du périphérique prévoit une destination à distance pour bob@example.call.ciscospark.com. Cisco Webex aborde cette situation en annulant ce segment d'appel en particulier.

Pour Cisco Webex correctement annuler le segment d'appel, Cisco Webex initialement requises pour a mis un jeu de paramètres dans le SIP en-tête laquelle il serait allure pour les annuler ce segment donné. Le paramètre que Cisco Webex insère dans l'invitation (INVITE) de SIP s'appelle « **call-type=squared** » et cette valeur est saisie dans l'en-tête de contact. Si cette valeur disparaît du message, Cisco Webex ne comprend pas comment annuler l'appel.

Compte tenu de cette information, vous pouvez examiner sous un autre angle le scénario présenté plus tôt, dans lequel l'application Cisco Webex de l'utilisateur recevait deux notifications (invites) lorsque Jonathan Robb, l'utilisateur de Cisco Webex, faisait un appel. Pour résoudre ce type de problème, il faut toujours recueillir de l'information de journalisation de diagnostic provenant d'Expressway-C et d'Expressway E. Comme point de départ, vous pouvez consulter les

journaux d'Expressway-E. Cela vous permettra de déterminer que l'invitation (INVITE) de SIP comprend la valeur **call-type=squared**. Cette valeur se trouve dans l'en-tête de la première invitation entrante de Cisco Webex. Cela fera en sorte que le pare-feu ne manipule pas le message de n'importe quelle façon. Ci-dessous est un échantillon de l'invitation (INVITE) arrivant sur l'Expressway-E dans ce scénario.

```
2017-09-19T14:01:48.140-04:00 amer-expressway01 tvcs: UTCtime="2017-09-19 18:01:48,140"
Module="network.sip" Level="DEBUG": Action="Received" Local-ip="172.16.2.2" Local-port="5062"
Src-ip="146.20.193.73" Src-port="40342" Msg-Hash="11658696457333185909"
SIPMSG:
|INVITE sip:pstojano-test@rtp.ciscotac.net SIP/2.0
Via: SIP/2.0/TLS 192.168.5.164:5062;branch=z9hG4bK564cd36d87f3417513c9b559dc666f71,SIP/2.0/TLS
127.0.0.1:5070;branch=z9hG4bK-3237-5c5060d07ecc546a0bb861ef52a5f507;rport=43306
Call-ID: 6bc0ca8210c0b48df69f38057ec1e48b@127.0.0.1
CSeq: 1 INVITE
Contact: "l2sip-UA" <sip:l2sip-UA@l2sip-cfa-01.wbx2.com:5062;transport=tls>;call-type=squared
<-- Webex inserted value
From: "Jonathan Robb"
```

```
;tag=540300020
```

```
To:
```

L'en-tête de contact comprend la valeur **call-type=squared**. À ce moment-là, l'appel doit s'acheminer sur l'Expressway vers la zone du serveur de traverse Webex Hybrid. Nous pouvons faire des recherches dans les journaux d'Expressway-E pour déterminer de quelle manière l'appel est envoyé de l'Expressway-E. Cela permettra de vérifier si l'Expressway-E manipule l'invitation d'une façon ou d'une autre.

```
2017-09-19T14:01:48.468-04:00 amer-expressway01 tvcs: UTCtime="2017-09-19 18:01:48,468"
Module="network.sip" Level="DEBUG": Action="Sent" Local-ip="192.168.1.6" Local-port="7003" Dst-
ip="192.168.1.5" Dst-port="26686" Msg-Hash="1847271284712495612"
SIPMSG:
INVITE sip:pstojano-test@rtp.ciscotac.net SIP/2.0
Via: SIP/2.0/TLS 192.168.1.6:7003;egress-
zone=HybridCallServiceTraversal;branch=z9hG4bKec916b02b6d469abad0a30b93753f4b0859;proxy-call-
id=d7372034-85d1-41f8-af84-dffed6d1a9a9;rport
Via: SIP/2.0/TLS 192.168.1.6:5073;branch=z9hG4bKd91699370129b4c10d09e269525de00c2;x-cisco-local-
service=nettle;received=192.168.1.6;rport=43119;ingress-zone=DefaultZone
Via: SIP/2.0/TLS 64.102.241.236:5061;egress-
zone=DefaultZone;branch=z9hG4bK52aac9a181192566e01b98ae0280bdff858.0e65cdfe078cabb269eecb6bce132
8be;proxy-call-id=ec51e8da-e1a3-4210-95c9-494d12debc8;received=172.16.2.2;rport=25016
Via: SIP/2.0/TLS
192.168.5.164:5062;branch=z9hG4bK564cd36d87f3417513c9b559dc666f71;received=146.20.193.73;rport=4
0342;ingress-zone=HybridCallServicesDNS
Via: SIP/2.0/TLS 127.0.0.1:5070;branch=z9hG4bK-3237-5c5060d07ecc546a0bb861ef52a5f507;rport=43306
Call-ID: 6bc0ca8210c0b48df69f38057ec1e48b@127.0.0.1
CSeq: 1 INVITE
Contact: <sip:192.168.1.6:5073;transport=tls> <-- Webex inserted value is now missing
From: "Jonathan Robb"
```

;tag=540300020

To:

Max-Forwards: 15

Route: <sip:cucm.rtp.ciscotac.net;lr>

À l'examen de l'invitation (SIP INVITE) qui est en cours d'envoi de l'Expressway-E à l'Expressway-C, vous observerez que l'en-tête ne comprend plus la valeur **call-type=squared**. Signalons aussi qu'à la ligne 4, comme vous pourrez le voir, vous pouvez voir que la zone de sortie (egress-zone) correspond à **HybridCallServiceTraversal**. Vous pouvez maintenant conclure que la raison pour laquelle l'application Cisco Webex reçoit une deuxième notification (invite) lorsqu'on l'appelle vient de la disparition, dans l'Expressway-E, de la balise **call-type=squared** qui était contenue dans l'en-tête de contact de l'invitation (INVITE) de SIP. Il faut maintenant répondre à la question de savoir ce qui pourrait faire disparaître l'information dans l'en-tête.

L'appel doit s'acheminer par la traverse de Hybrid Call Service qui est configurée dans l'Expressway. C'est donc un bon endroit pour commencer l'examen. Si vous avez xConfiguration, vous pouvez voir comment cette zone est configurée. Pour cerner la zone dans xConfiguration, il suffit d'utiliser le nom enregistré dans la ligne Via qui apparaît dans les journaux. Vous pouvez voir ci-dessus qu'elle s'appelle egress-zone=HybridCallServiceTraversal. Lorsque ce nom est imprimé dans la ligne Via de l'en-tête de SIP, les espaces sont supprimés. Sous l'angle de xConfiguration, le vrai nom comprendrait des espaces et serait formaté à la traverse d'Hybrid Call Service.

```
*c xConfiguration Zones Zone 7 TraversalServer Authentication Mode: "DoNotCheckCredentials"
*c xConfiguration Zones Zone 7 TraversalServer Authentication UserName: "hybridauth"
*c xConfiguration Zones Zone 7 TraversalServer Collaboration Edge: "Off"
*c xConfiguration Zones Zone 7 TraversalServer H323 H46019 Demultiplexing Mode: "Off"
*c xConfiguration Zones Zone 7 TraversalServer H323 Port: "6007"
*c xConfiguration Zones Zone 7 TraversalServer H323 Protocol: "Assent"
*c xConfiguration Zones Zone 7 TraversalServer Registrations: "Allow"
*c xConfiguration Zones Zone 7 TraversalServer SIP Media AesGcm Support: "Off"
*c xConfiguration Zones Zone 7 TraversalServer SIP Media Encryption Mode: "Auto"
*c xConfiguration Zones Zone 7 TraversalServer SIP Media ICE Support: "Off"
*c xConfiguration Zones Zone 7 TraversalServer SIP Multistream Mode: "On"
*c xConfiguration Zones Zone 7 TraversalServer SIP ParameterPreservation Mode: "Off" <--
Possible Suspect Value
*c xConfiguration Zones Zone 7 TraversalServer SIP Poison Mode: "Off"
*c xConfiguration Zones Zone 7 TraversalServer SIP Port: "7003"
*c xConfiguration Zones Zone 7 TraversalServer SIP PreloadedSipRoutes Accept: "On" <--
Possible Suspect Value
*c xConfiguration Zones Zone 7 TraversalServer SIP Protocol: "Assent"
*c xConfiguration Zones Zone 7 TraversalServer SIP TLS Verify Mode: "On"
*c xConfiguration Zones Zone 7 TraversalServer SIP TLS Verify Subject Name: "rtp12-tpdmz-118-
VCSC.rtp.ciscotac.net"
*c xConfiguration Zones Zone 7 TraversalServer SIP Transport: "TLS"
*c xConfiguration Zones Zone 7 TraversalServer TCPProbe KeepAliveInterval: "20"
*c xConfiguration Zones Zone 7 TraversalServer TCPProbe RetryCount: "5"
*c xConfiguration Zones Zone 7 TraversalServer TCPProbe RetryInterval: "2"
*c xConfiguration Zones Zone 7 TraversalServer UDPProbe KeepAliveInterval: "20"
*c xConfiguration Zones Zone 7 TraversalServer UDPProbe RetryCount: "5"
*c xConfiguration Zones Zone 7 TraversalServer UDPProbe RetryInterval: "2"
*c xConfiguration Zones Zone 7 Name: "Hybrid Call Service Traversal"
```

Grâce aux paramètres cernés dans la traverse Hybrid Call Service, vous pouvez faire des recherches pour repérer des paramètres se démarquant, par exemple :

- SIP PreloadedSIPRoutes Accept : On (activé)
- SIP ParameterPreservatoin Mode : Off (désactivé)

Dans l'interface Web d'un Expressway, vous pouvez consulter la définition de ces valeurs et leurs fonctions.

Preloaded SIP Routes support (prise en charge préétablie du routage de SIP)

Activez la prise en charge Preloaded SIP routes support (« On ») pour permettre à cette zone de traiter les demandes d'invitation de SIP comprenant un en-tête de routage.

Preloaded SIP routes support doit être désactivé (« Off ») si vous souhaitez que la zone rejette les demandes d'invitation de SIP avec un en-tête.

SIP parameter preservation (préservation des paramètres de SIP)

Déterminez si B2BUA de l'Expressway préserve ou modifie les paramètres des demandes de SIP acheminées par l'intermédiaire de cette zone.

« On » (activé) préserve les paramètres de contact et de l'URI de demande de SIP des demandes s'acheminant entre cette zone et B2BUA.

« Off » (désactivé) permet à B2BUA de réécrire au besoin les paramètres de contact et de l'URI de demande de SIP des demandes s'acheminant entre cette zone et B2BUA.

Suivant ces définitions, selon xConfiguration et compte tenu du fait que la valeur **call-type=squared** est placée dans l'en-tête « Contact » de l'invitation de SIP, vous pouvez conclure que la désactivation de la valeur de préservation du paramètre SIP dans la zone de traverse de Hybrid Call Service est la raison pour laquelle la balise est effacée, ce qui explique les deux notifications que reçoit l'application Cisco Webex.

Solution

Pour conserver le paramètre **call-type=squared** dans l'en-tête de contact de l'invitation (INVITE) de SIP, vous devez vous assurer que l'Expressways prenne en charge la préservation des paramètres de SIP pour toutes les zones qui participent au traitement de l'appel :

1. Ouvrez une session dans l'Expressway-E
2. Naviguez jusqu'à **Configuration > Zones > Zones**
3. Sélectionnez la zone qui est en cours d'utilisation pour le serveur de traverse d'Hybrid
4. Définissez la valeur de préservation des paramètres de SIP (SIP parameter preservation value) à **« On » (activé)**
5. Enregistrez les paramètres.

```
#####  
#####  
#####  
#####
```

Note: Dans ce scénario, c'est la zone de serveur de traverse Webex Hybrid qui était mal configurée. N'oubliez pas qu'il est tout à fait possible que la valeur de préservation des paramètres de SIP soit désactivée (réglée à « Off ») dans les zones client de traverse Webex Hybrid ou dans les zones voisines de CUCM. Ces deux configurations seraient effectuées sur l'Expressway-C. Si c'était le cas, vous pourriez vous attendre à ce que l'Expressway-E ait envoyé

la valeur **call-type=squared** à l'Expressway-C et qu'il ait été retiré par l'Expressway-C.

Sortant : Le site vers Cisco Webex

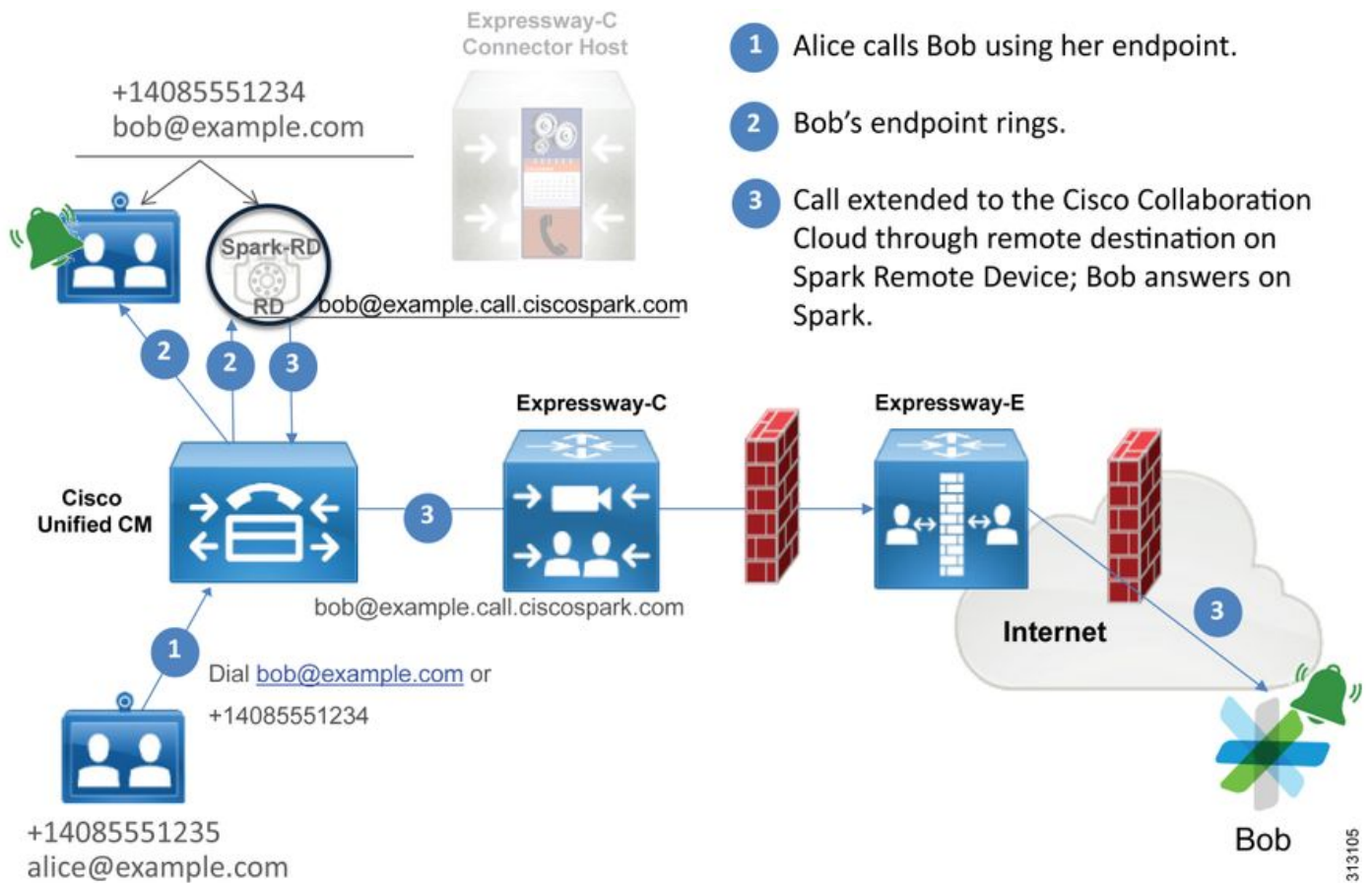
Presque tous les échecs d'une communication provenant d'un site à destination de Cisco Webex entraînent les mêmes symptômes déclarés : « Lorsque j'appelle un autre utilisateur activé dans Call Service Connect de mon téléphone enregistré auprès de Unified CM, son téléphone sonne, mais pas son application Cisco Webex. » Afin de résoudre ce genre de problématique, il est important de comprendre les flux d'appels et la logique s'appliquant lorsque ce type d'appel s'effectue.

Flux logique de haut niveau

1. L'utilisateur A lance un appel de son téléphone sur les lieux à l'URI de l'annuaire de l'utilisateur B
2. Le téléphone sur place de l'utilisateur B et CTI-RD/Webex-RD acceptent l'appel
3. Le téléphone sur place de l'utilisateur B commence à sonner
4. CTI-RD/Webex-RD de l'utilisateur B achemine cet appel vers la destination de `UserB@example.call.ciscopark.com`
5. Unified CM transmet cet appel à l'Expressway-C
6. L'Expressway-C envoie l'appel vers l'Expressway-E
7. L'Expressway-E effectue une recherche de DNS dans le domaine `callservice.ciscopark.com`
8. L'Expressway-E tente de se connecter à l'environnement Cisco Webex sur le port 5062
9. L'Expressway-E et l'environnement de Cisco Webex amorcent une prise de contact mutuelle
10. L'environnement de Cisco Webex parvient à passer l'appel sur l'application Cisco Webex disponible de l'utilisateur B
11. L'application disponible Cisco Webex de l'utilisateur B commence à sonner.

Flux d'appels

Naviguez jusqu'à **User B on-prem phone > Unified CM > CTI-RD/Webex-RD > Expressway-C > Expressway-E > Cisco Webex environment > Cisco Webex app** , comme l'indique l'image.



Note: L'image est tirée du [guide de conception Cisco Webex Hybrid](#).

Conseils pour l'analyse de journal

Si vos efforts de dépannage ont pour objet une situation dans laquelle des appels sortants acheminés vers Cisco Webex n'ont pas fonctionné correctement, vous souhaitez recueillir les journaux d'Unified CM, d'Expressway-C et d'Expressway-E. Ces ensembles de journaux vous permettront de vérifier comment l'appel est transmis à l'échelle de l'environnement. Une autre façon rapide de comprendre jusqu'où l'appel se déplace au sein de votre environnement sur place consiste à utiliser la fonction de l'historique de recherche (« Search History »). L'historique de recherche Expressway vous permettra de voir rapidement si l'appel acheminé vers Cisco Webex parvient à joindre l'Expressway-C ou l'Expressway-E.

Pour utiliser l'historique de recherche, vous pouvez suivre les étapes suivantes :

1. Ouvrez une session dans l'Expressway-E
Faites un appel de test
Naviguez jusqu'à **Status > Search History**
Vérifiez si vous consultez un appel qui a une adresse de destination de l' Webex uri de TYPE SIP qui devrait être appelé (user@example.call.ciscospark.com)
Si l'historique de recherche ne révèle pas que l'appel s'est rendu sur l'Expressway-E, répétez la démarche sur l'Expressway-C

Avant d'analyser les journaux de diagnostic sur l'Expressway, songez aux façons de cerner cet appel :

1. L'URI de demande de SIP sera l'adresse SIP de l'utilisateur de Cisco Webex
2. Le champ SIP FROM sera formaté pour que l'appelant soit répertorié comme « Prénom Nom » <sip:Alias@Domain>

Compte tenu de cette information, vous pouvez faire une recherche dans les journaux de diagnostic en fonction des paramètres suivants : URI de l'annuaire de la partie qui appelle, prénom et nom de la personne qui appelle ou adresse de SIP de Cisco Webex de la personne appelée. Si vous n'avez aucune de ces informations, vous pouvez effectuer une recherche sur "INVITE SIP :" qui localisera tous les appels SIP exécutés sur l'Expressway. Une fois que vous avez trouvé l'invitation de SIP de l'appel sortant, vous pouvez repérer et copier l'identifiant de l'appel SIP (SIP **Call-ID**). Une fois que vous avez cette donnée, vous pouvez simplement faire une recherche dans les journaux de diagnostic en fonction de l'identifiant de l'appel (Call-ID) pour voir tous les messages s'attachant à ce segment d'appel.

Voici quelques-uns des problèmes les plus courants observés avec des appels sortants d'un téléphone Unified CM à destination de l'environnement de Cisco Webex lorsque l'appel est destiné à un utilisateur qui est activé sur Call Service Connect.

Problème 1. Expressway ne peut pas résoudre l'adresse `callservice.ciscopark.com`

La procédure de fonctionnement standard pour une zone DNS d'Expressway consiste à effectuer une recherche de DNS de DNS fondée sur le domaine qui s'affiche à la droite de l'URI de demande. Pour expliquer cela, voici un exemple. Si la zone de DNS devait recevoir un appel comprenant l'URI de la demande `pstojano-test@dmzlab.call.ciscopark.com`, habituellement, la zone de DNS d'Expressway appliquerait la logique de recherche de SRV de DNS sur `dmzlab.call.ciscopark.com` , qui est à droite de l'URI de la demande. Si l'Expressway le faisait, vous pourriez vous attendre aux recherches et réponses que voici.

```
_sips._tcp.dmzlab.call.ciscopark.com.  
Response: 5 10 5061 l2sip-cfa-01.wbx2.com.  
l2sip-cfa-01.wbx2.com  
Response: 146.20.193.64
```

Un examen attentif permet de constater que la réponse de SRV est une adresse de serveur et le port 5061, plutôt que 5062.

Cela signifie que la prise de contact mutuelle de TLS qui se produit sur le port 5062 ne sera pas complétée et qu'un port distinct est utilisé pour la signalisation entre Expressway et Cisco Webex. Voici le défi lié à cette situation : le *guide de déploiement de Cisco Webex Hybrid Call Services* n'aborde pas explicitement l'utilisation du port 5061 parce que certains environnements ne permettent pas les appels interentreprises.

Voici comment contourner cette logique de recherche de SRV dans la zone de DNS : il faut configurer l'Expressway de façon à ce qu'aient lieu des recherches explicites selon une valeur que vous précisez.

Maintenant, dans notre analyse de cet appel en particulier, vous pouvez mettre l'accent sur l'Expressway-E, car vous avez déterminé (au moyen de l'historique de recherche) que l'appel s'est rendu jusque-là. Commencez par la première invitation de SIP (SIP INVITE) se présentant dans l'Expressway-E pour vérifier de quelle zone elle provenait et quelles étaient les règles de recherche appliquées, la zone vers laquelle l'appel se dirigeait et (si l'appel s'est correctement acheminé vers la zone DNS) la logique de recherche de DNS mise en œuvre.

Module="network.sip" Level="DEBUG": Action="Received" Local-ip="192.168.1.6" Local-port="7003"
Src-ip="192.168.1.5" Src-port="26686" Msg-Hash="4341754241544006348"

SIPMSG:

|**INVITE sip:pstojano-test@dmzlab.call.ciscospark.com** SIP/2.0

Via: SIP/2.0/TLS 192.168.1.5:5061;**egress-**
zone=HybridCallServiceTraversal;branch=z9hG4bK6d734eaf7a6d733bd1e79705b7445ebb46175.1d33be65c99c
56898f85df813f1db3a7;proxy-call-id=47454c92-2b30-414a-b7fe-aff531296bcf;rport

Via: SIP/2.0/TCP 192.168.1.21:5065;branch=z9hG4bK13187594dd412;received=192.168.1.21;ingress-
zone=CUCM11

Call-ID: 991f7e80-9c11517a-130ac-1501a8c0@192.168.1.21

CSeq: 101 INVITE

Call-Info: <urn:x-cisco-remotecallinfo>;x-cisco-video-traffic-class=DESKTOP

Remote-Party-ID: "Jonathan Robb"

<sip:5010@rtp.ciscotac.net>;party=calling;screen=yes;privacy=off

Contact: <sip:5010@192.168.1.21:5065;transport=tcp>;video;audio

From: "Jonathan Robb"

;tag=332677~c9cc7ddc-9592-49e8-a13c-79e26f48eebc-30106860

To:

Max-Forwards: 15

Record-Route: <sip:proxy-call-id=47454c92-2b30-414a-b7fe-
aff531296bcf@192.168.1.5:5061;transport=tls;lr>

Record-Route: <sip:proxy-call-id=47454c92-2b30-414a-b7fe-
aff531296bcf@192.168.1.5:5060;transport=tcp;lr>

Allow: INVITE, OPTIONS, INFO, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE, NOTIFY

User-Agent: Cisco-CUCM11.5

Expires: 180

Date: Tue, 19 Sep 2017 17:18:50 GMT

Supported: timer, resource-priority, replaces, X-cisco-srtp-fallback, X-cisco-original-called

Session-Expires: 1800

Min-SE: 1800

Allow-Events: presence

X-TAATag: 2272025a-ce36-49d0-8d93-cb6a5e90ffe0

Session-ID: 75957d4fb66a13e835c10737aa332675;remote=00000000000000000000000000000000

Cisco-Guid: 2568978048-0000065536-000000148-0352430272

Content-Type: application/sdp

Content-Length: 714

<SDP Omitted>

Dans cette invitation SIP, vous pouvez rassembler l'URI de demande (pstojano-test@dmzlab.call.ciscospark.com), l'**ID d'appel** (991f7e80-9c11517a-130ac-1501a8c0), **De** (« Jonathan Robb » <sip:5010@rtp.ciscotac.net>), **To** (sip:pstojano-test@dmzlab.call.ciscospark.com) et **User-Agent** (Cisco-CUCM11.5). Une fois que l'invitation est reçue, l'Expressway doit prendre des décisions logiques pour déterminer s'il est possible d'acheminer l'appel vers une autre zone. L'Expressway le fait selon des règles de recherche.

2017-09-19T13:18:50.564-04:00 amer-expressway01 tvcs: UTCtime="2017-09-19 17:18:50,564"

Module="network.search" Level="DEBUG": **Detail="Search rule 'B2B calls to VCS-C' did not match destination alias 'pstojano-test@dmzlab.call.ciscospark.com' "**

2017-09-19T13:18:50.564-04:00 amer-expressway01 tvcs: UTCtime="2017-09-19 17:18:50,564"

Module="network.search" Level="DEBUG": **Detail="Search rule 'Webex Hybrid' ignored due to source filtering"**

2017-09-19T13:18:50.564-04:00 amer-expressway01 tvcs: UTCtime="2017-09-19 17:18:50,564"

Module="network.search" Level="DEBUG": Detail="Search rule 'Calls to Webex' did not match destination alias 'pstojano-test@dmzlab.call.ciscospark.com'"

2017-09-19T13:18:50.564-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 17:18:50,564"

Module="network.search" Level="DEBUG": Detail="Considering search rule 'Webex Hybrid - to Webex Cloud' towards target 'Hybrid Call Services DNS' at priority '90' with alias 'pstojano-test@dmzlab.call.ciscospark.com'"

Selon l'extrait du registre ci-dessus, vous pouvez voir que l'Expressway-E a parcouru quatre règles de recherche, mais que seule la règle (Webex Hybrid - to Webex Cloud) a été envisagée. La règle de recherche était assortie à une priorité de 90 et ciblait la destination suivante : la zone DNS d'Hybrid Call Services Maintenant que l'appel est envoyé à la zone DNS, vous pouvez passer en revue les recherches SRV de DNS qui se produisent sur l'Expressway-E

2017-09-19T13:18:50.565-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 17:18:50,565"

Module="network.dns" Level="DEBUG": Detail="Sending DNS query"

Name="dmzlab.call.ciscospark.com" Type="NAPTR (IPv4 and IPv6)"

2017-09-19T13:18:50.718-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 17:18:50,718"

Module="network.dns" Level="DEBUG": Detail="Sending DNS query"

Name="_sips._tcp.dmzlab.call.ciscospark.com" Type="SRV (IPv4 and IPv6)"

2017-09-19T13:18:50.795-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 17:18:50,795"

Module="network.dns" Level="DEBUG": Detail="Resolved hostname to:

['IPv4' 'TCP' '146.20.193.64:5061'] (A/AAAA) Hostname:'l2sip-cfa-01.wbx2.com' Port:'5061'

Priority:'5' TTL:'300' Weight:'10' (SRV) Number of relevant records retrieved: 2"

Dans l'extrait ci-dessus, vous pouvez voir que l'Expressway-E a effectué la recherche SRV en se basant sur le côté droit de l'URI de requête (_sips._tcp.dmzlab.call.ciscospark.com) et qu'il s'est résolu en un nom d'hôte de l2sip-cfa-01.wbx2.com et port 50661. Le nom d'hôte l2sip-cfa-01.wbx2.com correspond à 146.20.193.64. Compte tenu de ce qui précède, la prochaine étape logique dans Expressway consiste à envoyer un paquet SYN de TCP pour 146.20.193.64 afin de tenter d'établir l'appel. Dans le journal de l'Expressway-E, vous pouvez vérifier si ça se produit.

2017-09-19T13:18:51.145-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 17:18:51,145"

Module="network.tcp" Level="DEBUG": Src-ip="172.16.2.2" Src-port="25010" Dst-ip="146.20.193.64" Dst-port="5061" Detail="TCP Connecting"

2017-09-19T13:19:01.295-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 17:19:01,289"

Module="network.tcp" Level="ERROR": Src-ip="172.16.2.2" Src-port="25010" Dst-ip="146.20.193.64" Dst-port="5061" Detail="TCP Connection Failed"

Dans l'extrait de journalisation de diagnostic d'Expressway-E, vous pouvez voir que l'Expressway-E tente de se connecter à l'IP 146.20.193.64 qui a précédemment été résolue sur le port 5061 de TCP. Toutefois, cette connexion échoue clairement. Il est possible d'observer la même chose dans les captures de paquets recueillies.

Expressway-E attempts TCP Connection

No.	Time	Source	Destination	Protocol	S Port	D Port	Length	Info
3878	2017-09-19 17:18:08.801765	68.67.59.22	172.16.2.2	TCP	25876	5061	66	25876->5061 [FIN, ACK] Seq=1 Ack=1 win=36 Len=0 Tsva1=231154828 TSecr=4109470239
3879	2017-09-19 17:18:08.801929	172.16.2.2	68.67.59.22	TCP	5061	25876	66	5061->25876 [FIN, ACK] Seq=1 Ack=2 win=36 Len=0 Tsva1=311465862 TSecr=231154828
3882	2017-09-19 17:18:08.822153	68.67.59.22	172.16.2.2	TCP	25876	5061	66	25876->5061 [ACK] Seq=2 Ack=2 win=362 Len=0 Tsva1=231154849 TSecr=4111465862
8109	2017-09-19 17:18:25.110830	192.33.146.113	172.16.2.2	TCP	50714	5061	60	50714->5061 [RST, ACK] Seq=1 Ack=1 win=312 Len=0
14878	2017-09-19 17:18:51.145472	172.16.2.2	146.20.193.64	TCP	25010	5061	74	25010->5061 [SYN] Seq=0 win=29200 Len=0 MSS=1460 SACK_PERM=1 Tsva1=314491012 TSecr=0 ws=128
15158	2017-09-19 17:18:52.203326	172.16.2.2	146.20.193.64	TCP	25010	5061	74	[TCP Retransmission] 25010->5061 [SYN] Seq=0 win=29200 Len=0 MSS=1460 SACK_PERM=1 Tsva1=314
15162	2017-09-19 17:18:52.203324	172.16.2.2	146.20.193.64	TCP	25010	5061	74	[TCP Retransmission] 25010->5061 [SYN] Seq=0 win=29200 Len=0 MSS=1460 SACK_PERM=1 Tsva1=314
15170	2017-09-19 17:18:55.283328	172.16.2.2	146.20.193.64	TCP	25010	5061	74	[TCP Retransmission] 25010->5061 [SYN] Seq=0 win=29200 Len=0 MSS=1460 SACK_PERM=1 Tsva1=314
15377	2017-09-19 17:19:01.328621	172.16.2.2	146.20.193.64	TCP	25011	5061	74	25011->5061 [SYN] Seq=0 win=29200 Len=0 MSS=1460 SACK_PERM=1 Tsva1=314501195 TSecr=0 ws=128
15846	2017-09-19 17:19:02.379327	172.16.2.2	146.20.193.64	TCP	25011	5061	74	[TCP Retransmission] 25011->5061 [SYN] Seq=0 win=29200 Len=0 MSS=1460 SACK_PERM=1 Tsva1=314
18425	2017-09-19 17:19:04.427323	172.16.2.2	146.20.193.64	TCP	25011	5061	74	[TCP Retransmission] 25011->5061 [SYN] Seq=0 win=29200 Len=0 MSS=1460 SACK_PERM=1 Tsva1=314
19459	2017-09-19 17:19:08.439332	172.16.2.2	146.20.193.64	TCP	25011	5061	74	[TCP Retransmission] 25011->5061 [SYN] Seq=0 win=29200 Len=0 MSS=1460 SACK_PERM=1 Tsva1=314

The Expressway-E doesn't receive a SYN-ACK so it retries the SYN packet again 3 times

Selon ces résultats, il est évident que le trafic sur le port 5061 n'est pas fructueux. Toutefois, Hybrid Call Service Connect visait l'utilisation du port TCP 5062, plutôt que 5061. Par conséquent, vous devez songer à la question de savoir pourquoi l'Expressway-E ne parvient pas à effectuer un enregistrement de SRV qui devrait s'associer au port 5062. Pour tenter de répondre à cette

question, vous pouvez examiner les éventuels problèmes de configuration dans la zone DNS de WebexHybrid sur l'Expressway-E.

```
*c xConfiguration Zones Zone 6 Name: "Hybrid Call Services DNS"
*c xConfiguration Zones Zone 6 DNS SIP Authentication Trust Mode: "Off"
*c xConfiguration Zones Zone 6 DNS SIP Default Transport: "TLS"
*c xConfiguration Zones Zone 6 DNS SIP DnsOverride Name: "ciscopark.com"
*c xConfiguration Zones Zone 6 DNS SIP DnsOverride Override: "Off"
*c xConfiguration Zones Zone 6 DNS SIP Media AesGcm Support: "Off"
*c xConfiguration Zones Zone 6 DNS SIP Media Encryption Mode: "On"
*c xConfiguration Zones Zone 6 DNS SIP Media ICE Support: "Off"
*c xConfiguration Zones Zone 6 DNS SIP ParameterPreservation Mode: "Off"
*c xConfiguration Zones Zone 6 DNS SIP Poison Mode: "Off"
*c xConfiguration Zones Zone 6 DNS SIP PreloadedSipRoutes Accept: "On"
*c xConfiguration Zones Zone 6 DNS SIP Record Route Address Type: "IP"
*c xConfiguration Zones Zone 6 DNS SIP SearchAutoResponse: "Off"
*c xConfiguration Zones Zone 6 DNS SIP TLS Verify InboundClassification: "On"
*c xConfiguration Zones Zone 6 DNS SIP TLS Verify Mode: "On"
*c xConfiguration Zones Zone 6 DNS SIP TLS Verify Subject Name: "callservice.ciscopark.com"
*c xConfiguration Zones Zone 6 DNS SIP UDP BFCP Filter Mode: "Off"
*c xConfiguration Zones Zone 6 DNS SIP UDP IX Filter Mode: "Off"
```

Dans xConfiguration de l'Expressway-E, vous pouvez voir que deux valeurs particulières se rattachent aux recherches de DNS : **DNSOverride Name** et **DNSOverride Override**. Selon xConfiguration, il appert que la fonction de remplacement DNSOverride Override est désactivée (« Off ») et par conséquent, la fonction DNSOverride Name ne peut pas s'appliquer. Pour mieux comprendre les fonctions de ces valeurs, vous pouvez utiliser l'interface Web de l'Expressway pour obtenir la définition de ces valeurs.

Modify DNS request (devient DnsOverride Override dans xConfig)

Permet de diriger les appels sortants SIP provenant de cette zone à un domaine SIP précisé manuellement au lieu du domaine de la destination de composition. Cette option est principalement conçu pour une utilisation avec Cisco Webex Call Service. Consultez la section www.cisco.com/go/hybrid-services.

Domain to search for (devient DnsOverride Name dans xConfig)

Saisissez un FQDN à trouver dans DNS au lieu de chercher le domaine dans l'URI de SIP des appels sortants. Cela n'a pas d'incidence sur l'URI de SIP original.

Maintenant que vous avez accès à ces définitions, il ne fait aucun doute que ces valeurs, si elles sont correctement définies, sont entièrement pertinentes pour notre logique de recherche de DNS. Si vous associez cela aux instructions du Guide de déploiement pour les services d'appel hybrides Cisco Webex, vous constaterez que la demande de modification DNS doit être définie sur **On** et que le domaine à rechercher doit être défini sur **callservice.ciscopark.com**. Si vous changez ces valeurs afin qu'elles précisent la bonne information, la logique de la recherche de SRV de DNS serait complètement différente. Voici un extrait de ce qui pourrait se produire, sous l'angle de la journalisation de diagnostic d'Expressway-E

```
2017-09-19T10:18:35.048-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 14:18:35,048"
Module="network.dns" Level="DEBUG": Detail="Sending DNS query"
Name="_sips._tcp.callservice.ciscopark.com" Type="SRV (IPv4 and IPv6)"
2017-09-19T10:18:35.126-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 14:18:35,126"
Module="network.dns" Level="DEBUG": Detail="Resolved hostname to:
['IPv4' 'TCP' '146.20.193.70:5062'] (A/AAAA) ['IPv4' 'TCP' '146.20.193.64:5062'] (A/AAAA)
```



```
Hostname: 'l2sip-cfa-02.wbx2.com' Port: '5062' Priority: '5' TTL: '300' Weight: '10' (SRV)
Hostname: 'l2sip-cfa-01.wbx2.com' Port: '5062' Priority: '5' TTL: '300' Weight: '10' (SRV) Number of
relevant records retrieved: 4"
```

Solution

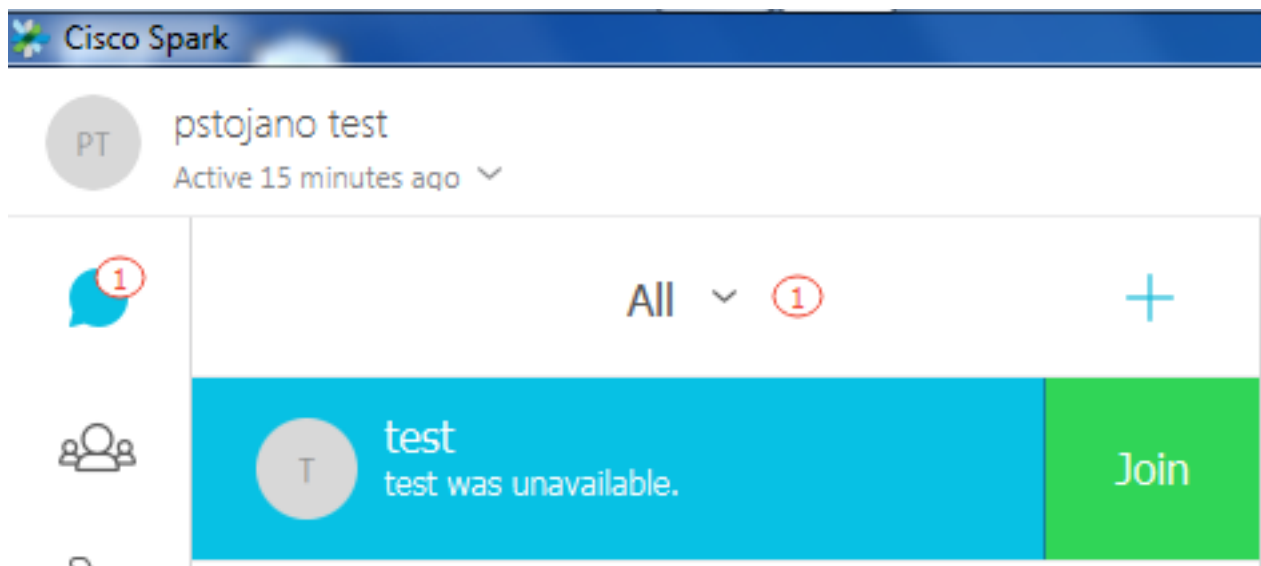
1. Ouvrez une session dans l'Expressway-E
2. Naviguez jusqu'à **Configuration > Zones > Zones**
3. Sélectionnez la zone de DNS Webex Hybrid qui a été configurée
4. Activez la demande de modification de DNS (Modify DNS) (en la réglant à « **On** »)
5. Définissez le domaine dans lequel faire la recherche de valeur (Domain to search for value) à **callservice.ciscopark.com**
6. Enregistrez les modifications

Note: S'il n'y a qu'une zone de DNS en cours d'utilisation sur l'Expressway, il faudrait configurer une zone DNS distincte pour utilisation avec Hybrid Call Service, afin de tirer parti de ces valeurs.

Problème 2. Le port 5062 est bloqué en sortie vers Cisco Webex

Un aspect unique des échecs des appels sortants acheminés vers Cisco Webex est que l'application Cisco Webex de la partie appelée affichera un bouton Join pour se joindre à l'appel dans son interface même si le client ne sonne jamais. Comme nous l'avons vu dans le scénario ci-dessus, pour ce problème, vous devrez de nouveau utiliser les mêmes outils et rapports de journalisation pour mieux comprendre où la défaillance est survenue. Pour obtenir des conseils sur la façon d'isoler des problèmes liés aux appels et d'analyser les journaux, consultez la section de cet article, tel que le montre l'image.

Illustration du bouton pour se joindre qui apparaît



Un peu comme pour le problème n° 1 des appels sortants, vous pouvez commencer par analyser les journaux de diagnostic de l'Expressway-E, car vous avez utilisé l'historique de recherche de l'Expressway afin de déterminer que l'appel s'est rendu jusque-là. Comme précédemment, commencez par l'invitation initiale qui arrive dans l'Expressway-E à partir de l'Expressway-C. N'oubliez pas que vous devez rechercher les éléments suivants :

1. Est-ce que l'Expressway-E reçoit l'invitation (INVITE)

2. Est-ce que la logique des règles de recherche permet l'acheminement de l'appel dans la zone DNS d'Hybrid
3. Est-ce que la zone de DNS effectue la recherche de DNS dans le bon domaine
4. Est-ce que le système a tenté une prise de contact mutuelle de TCP sur le port 5062 et est-ce qu'il est parvenu à l'établir
5. Est-ce que la prise de contact mutuelle de TLS s'est révélée fructueuse

```
2017-09-19T10:18:35.023-04:00 amer-expressway01 tvcs: UTCtime="2017-09-19 14:18:35,017"
Module="network.sip" Level="DEBUG": Action="Received" Local-ip="192.168.1.6" Local-port="7003"
Src-ip="192.168.1.5" Src-port="26513" Msg-Hash="3732376649380137405"
SIPMSG:
|INVITE sip:pstojano-test@dmzlab.call.ciscopark.com SIP/2.0
Via: SIP/2.0/TLS 192.168.1.5:5061;egress-
zone=HybridCallServiceTraversal;branch=z9hG4bK57d8d5c823824bcd62f6ff7e09f9939482.899441b6d60c
444e4ed58951d07b5224;proxy-call-id=696f6f1c-9abe-47f3-96a4-e26f649fb76f;rport
Via: SIP/2.0/TCP 192.168.1.21:5065;branch=z9hG4bK12d4b77c97a64;received=192.168.1.21;ingress-
zone=CUCM11
Call-ID: 6a48de80-9c11273a-12d08-1501a8c0@192.168.1.21
CSeq: 101 INVITE
Call-Info: <urn:x-cisco-remotecallinfo>;x-cisco-video-traffic-class=DESKTOP
Remote-Party-ID: "Jonathan Robb"
<sip:5010@rtp.ciscotac.net>;party=calling;screen=yes;privacy=off
Contact: <sip:5010@192.168.1.21:5065;transport=tcp>;video;audio
From: "Jonathan Robb"

;tag=328867~c9cc7ddc-9592-49e8-a13c-79e26f48eebc-30106829
To:

Max-Forwards: 15
Record-Route: <sip:proxy-call-id=696f6f1c-9abe-47f3-96a4-
e26f649fb76f@192.168.1.5:5061;transport=tls;lr>
Record-Route: <sip:proxy-call-id=696f6f1c-9abe-47f3-96a4-
e26f649fb76f@192.168.1.5:5060;transport=tcp;lr>
Allow: INVITE, OPTIONS, INFO, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE, NOTIFY
User-Agent: Cisco-CUCM11.5
Expires: 180
Date: Tue, 19 Sep 2017 14:18:34 GMT
Supported: timer, resource-priority, replaces, X-cisco-srtp-fallback, X-cisco-original-called
Session-Expires: 1800
Min-SE: 1800
Allow-Events: presence
X-TAATag: b2967a3b-93fb-4ca4-b0d7-131f75335684
Session-ID: 75957d4fb66a13e835c10737aa328865;remote=00000000000000000000000000000000
Cisco-Guid: 1783160448-0000065536-000000126-0352430272
Content-Type: application/sdp
Content-Length: 714
<SDP Omitted>
```

Comme vous pouvez le voir dans l'invitation (INVITE) ci-dessus, l'invitation reçue est normale. Il s'agit d' une action de réception qui provient de l'adresse IP d'Expressway-C. Vous pouvez désormais passer à la logique des règles de recherche

```

2017-09-19T10:18:35.023-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 14:18:35,022"
Module="network.search" Level="DEBUG": Detail="Search rule 'B2B calls to VCS-C' did not match
destination alias 'pstojano-test@dmzlab.call.ciscospark.com'"
2017-09-19T10:18:35.023-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 14:18:35,022"
Module="network.search" Level="DEBUG": Detail="Search rule 'Webex Hybrid' ignored due to source
filtering"
2017-09-19T10:18:35.023-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 14:18:35,022"
Module="network.search" Level="DEBUG": Detail="Search rule 'Calls to Webex' did not match
destination alias 'pstojano-test@dmzlab.call.ciscospark.com'"
2017-09-19T10:18:35.023-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 14:18:35,022"
Module="network.search" Level="DEBUG": Detail="Considering search rule 'Webex Hybrid - to Webex
Cloud' towards target 'Hybrid Call Services DNS' at priority '90' with alias 'pstojano-
test@dmzlab.call.ciscospark.com'"

```

En vous basant sur l'extrait de journal ci-dessus, vous pouvez voir que l'Expressway-E a analysé quatre règles de recherche, mais une seule (*Webex Hybrid - vers Webex Cloud*) a été pris en considération. La règle de recherche avait une priorité de 90 et visait à accéder à la *Zone DNS Hybrid Call Services*. Maintenant que l'appel est envoyé à la zone DNS, vous pouvez passer en revue les recherches SRV de DNS qui se produisent sur l'Expressway-E C'est parfaitement normal. Maintenant, avez votre examen sur la logique de la recherche de DNS

```

2017-09-19T10:18:35.048-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 14:18:35,048"
Module="network.dns" Level="DEBUG": Detail="Sending DNS query"
Name="_sips._tcp.callservice.ciscospark.com" Type="SRV (IPv4 and IPv6)"
2017-09-19T10:18:35.126-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 14:18:35,126"
Module="network.dns" Level="DEBUG": Detail="Resolved hostname to:
['IPv4 'TCP' '146.20.193.70:5062'] (A/AAAA) ['IPv4 'TCP' '146.20.193.64:5062'] (A/AAAA)
Hostname:'l2sip-cfa-02.wbx2.com' Port:'5062' Priority:'5' TTL:'300' Weight:'10' (SRV)
Hostname:'l2sip-cfa-01.wbx2.com' Port:'5062' Priority:'5' TTL:'300' Weight:'10' (SRV) Number of
relevant records retrieved: 4"

```

Vous pouvez clairement voir que dans ce cas-ci, l'enregistrement SRV callservice.ciscospark.com est envoyé. La réponse a pour objet quatre différents enregistrements valides qui utilisent tous le port 5062. Ceci est un comportement normal. À ce stade-ci, vous pouvez analyser la prise de contact mutuelle de TCP qui devrait suivre ensuite. Comme il en a été question plus tôt, vous pouvez faire dans les journaux de diagnostic des recherches qui ont pour objet la connexion TCP (« TCP Connecting »). Cherchez à repérer la ligne qui comprend Dst-port="5062". Voici un exemple de ce que vous verrez dans ce scénario :

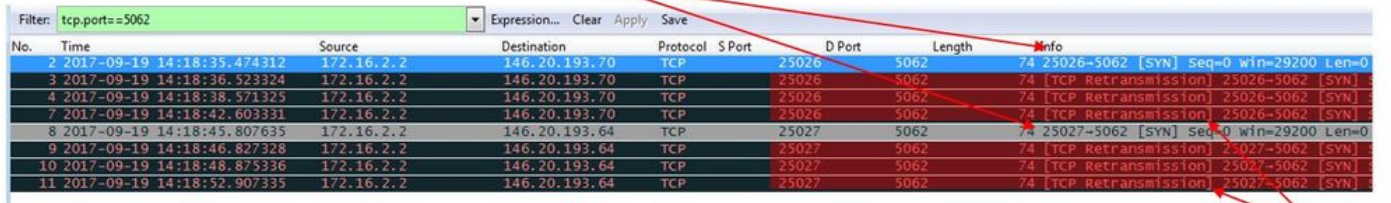
```

2017-09-19T10:18:35.474-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 14:18:35,474"
Module="network.tcp" Level="DEBUG": Src-ip="172.16.2.2" Src-port="25026" Dst-ip="146.20.193.70"
Dst-port="5062" Detail="TCP Connecting"
2017-09-19T10:28:35.295-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 14:28:35,289"
Module="network.tcp" Level="ERROR": Src-ip="172.16.2.2" Src-port="25026" Dst-ip="146.20.193.70"
Dst-port="5062" Detail="TCP Connection Failed"

```

Vous pouvez également utiliser tcpdump qui fait partie du groupe de journalisation de diagnostic afin d'obtenir de plus amples renseignements sur la prise de contact mutuelle de TCP, comme l'indique l'image.

Expressway-E attempts TCP Connection twice



No.	Time	Source	Destination	Protocol	S Port	D Port	Length	Info
2	2017-09-19 14:18:35.474312	172.16.2.2	146.20.193.70	TCP	25026	5062	74	25026->5062 [SYN] Seq=0 win=29200 Len=0
3	2017-09-19 14:18:36.523324	172.16.2.2	146.20.193.70	TCP	25026	5062	74	[TCP Retransmission] 25026->5062 [SYN]
4	2017-09-19 14:18:38.571325	172.16.2.2	146.20.193.70	TCP	25026	5062	74	[TCP Retransmission] 25026->5062 [SYN]
7	2017-09-19 14:18:42.603331	172.16.2.2	146.20.193.70	TCP	25026	5062	74	[TCP Retransmission] 25026->5062 [SYN]
8	2017-09-19 14:18:45.807635	172.16.2.2	146.20.193.64	TCP	25027	5062	74	25027->5062 [SYN] Seq=0 win=29200 Len=0
9	2017-09-19 14:18:46.827328	172.16.2.2	146.20.193.64	TCP	25027	5062	74	[TCP Retransmission] 25027->5062 [SYN]
10	2017-09-19 14:18:48.875336	172.16.2.2	146.20.193.64	TCP	25027	5062	74	[TCP Retransmission] 25027->5062 [SYN]
11	2017-09-19 14:18:52.907335	172.16.2.2	146.20.193.64	TCP	25027	5062	74	[TCP Retransmission] 25027->5062 [SYN]

The Expressway-E doesn't receive a SYN-ACK so it attempts to retransmit.

À ce stade, vous pouvez conclure que l'Expressway-E achemine correctement l'appel. Dans ce scénario, le défi vient de ce qu'une connexion TCP ne peut pas être établie dans l'environnement de Webex. Cela pourrait s'attribuer au fait que l'environnement de Webex ne répond pas aux paquets SYN de TCP. Toutefois, c'est peu probable, car le serveur traitant la connexion est partagé entre un grand nombre de clients. Il est plus probable que certains types de périphériques intermédiaires (pare-feu, IPS, etc.) ne permettent pas l'acheminement externe du trafic.

Solution

Parce que le problème était isolé, ces données doivent être communiquées à l'administrateur réseau du client. De plus, s'il a besoin de plus amples renseignements, vous pouvez prendre une capture de l'interface externe de l'appareil en périphérie ou du pare-feu en guise de preuves supplémentaires. Sous l'angle d'Expressway, il n'y a aucune autre action à effectuer, car le problème ne se situe pas sur ce périphérique.

Problème 3. Erreur de configuration de la règle de recherche Expressway

Les erreurs de configuration de la règle de recherche sont au nombre des problèmes de configuration les plus répandus pour les Expressways. Les problèmes de configuration de la règle de la recherche peuvent être bidirectionnels, car vous avez besoin de règles de recherche pour les appels entrants et pour les appels sortants. Tandis que vous parcourez le problème, vous découvrirez que si les problèmes de Regex sont assez courants sur l'Expressway, ils ne sont pas toujours la cause d'un problème de règle de recherche. Dans ce segment en particulier, vous examinerez un appel sortant en défaillance. Comme dans tous nos autres scénarios d'appels sortants acheminés, les symptômes demeurent identiques :

- L'application Cisco Webex de l'utilisateur appelé fait apparaître un bouton pour se joindre à l'appel (Join)
- Le téléphone qui fait l'appel émet une tonalité de rappel
- Le téléphone sur les lieux de l'utilisateur appelé sonne
- L'application Cisco Webex de l'utilisateur appelé n'a jamais sonné

Comme dans tous les autres scénarios, vous voudrez tirer parti des traces de SDL de CUCM, de même que des rapports de journalisation de diagnostic de l'Expressway-C et de l'Expressway-E. Comme dans les autres cas, vous devrez faire appel à l'historique de recherche et aux conseils connexes pour repérer l'appel dans les journaux de diagnostic. De nouveau, au moyen de l'historique de recherche de l'Expressway-E, il est déterminé que l'appel était en train de s'y rendre lorsqu'il a défailli. Vous trouverez ci-dessous le début de l'analyse permettant d'examiner l'invitation de SIP arrivant dans l'Expressway-E en provenance de l'Expressway-C.

```
2017-09-25T11:26:02.959-04:00 amer-expressway01 tvcs: UTCTime="2017-09-25 15:26:02,959"
Module="network.sip" Level="DEBUG": Action="Received" Local-ip="192.168.1.6" Local-port="7003"
Src-ip="192.168.1.5" Src-port="25675" Msg-Hash="1536984498381728689"
SIPMSG:
|INVITE sip:pstojano-test@dmzlab.call.ciscospark.com SIP/2.0
Via: SIP/2.0/TLS 192.168.1.5:5061;egress-
zone=HybridCallServiceTraversal;branch=z9hG4bK1c7bf93ff08014ca5e00bb0b5f8b184b272412.a81f2992e38
63ac202a000a3dd599763;proxy-call-id=f79b8631-947b-46d4-a888-911bf0150bfe;rport
Via: SIP/2.0/TCP 192.168.1.21:5065;branch=z9hG4bK1c8c419938648;received=192.168.1.21;ingress-
zone=CUCM11
Call-ID: d58f2680-9c91200a-1c7ba-1501a8c0@192.168.1.21
CSeq: 101 INVITE
Call-Info: <urn:x-cisco-remotecallinfo>;x-cisco-video-traffic-class=DESKTOP
Remote-Party-ID: "Jonathan Robb"
```

<sip:5010@rtp.ciscotac.net>;party=calling;screen=yes;privacy=off
Contact: <sip:5010@192.168.1.21:5065;transport=tcp>;video;audio
From: "Jonathan Robb"

tag=505817~c9cc7ddc-9592-49e8-a13c-79e26f48eebc-30106972

To:

Max-Forwards: 15
Record-Route: <sip:proxy-call-id=f79b8631-947b-46d4-a888-911bf0150bfe@192.168.1.5:5061;transport=tls;lr>
Record-Route: <sip:proxy-call-id=f79b8631-947b-46d4-a888-911bf0150bfe@192.168.1.5:5060;transport=tcp;lr>
Allow: INVITE, OPTIONS, INFO, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE, NOTIFY
User-Agent: Cisco-CUCM11.5
Expires: 180
Date: Mon, 25 Sep 2017 15:26:02 GMT
Supported: timer, resource-priority, replaces, X-cisco-srtp-fallback, X-cisco-original-called
Session-Expires: 1800
Min-SE: 1800
Allow-Events: presence
X-TAATag: 8e8c014d-5d01-4581-8108-5cb096778fc5
Session-ID: 75957d4fb66a13e835c10737aa505813;remote=00000000000000000000000000000000
Cisco-Guid: 3582928512-0000065536-0000000240-0352430272
Content-Type: application/sdp
Content-Length: 714

<SDP Omitted>

À l'aide de l'ID d'appel (**d58f2680-9c91200a-1c7ba-1501a8c0**) à partir de l'en-tête SIP, vous pouvez rapidement rechercher tous les messages associés à cette boîte de dialogue. Lorsque vous consultez la troisième occurrence dans les journaux pour ce Call-ID, vous pouvez voir que l'Expressway-E envoie immédiatement une erreur **04 Not Found** à l'Expressway-C.

2017-09-25T11:26:13.286-04:00 amer-expressway01 tvcs: UTCtime="2017-09-25 15:26:13,286"
Module="network.sip" Level="DEBUG": **Action="Sent"** Local-ip="192.168.1.6" Local-port="7003" Dst-ip="192.168.1.5" Dst-port="25675" Msg-Hash="12372154521012287279"

SIPMSG:

|SIP/2.0 404 Not Found

Via: SIP/2.0/TLS 192.168.1.5:5061;egress-zone=HybridCallServiceTraversal;branch=z9hG4bK1c7bf93ff08014ca5e00bb0b5f8b184b272412.a81f2992e3863ac202a000a3dd599763;proxy-call-id=f79b8631-947b-46d4-a888-911bf0150bfe;received=192.168.1.5;rport=25675;ingress-zone=HybridCallServiceTraversal

Via: SIP/2.0/TCP 192.168.1.21:5065;branch=z9hG4bK1c8c419938648;received=192.168.1.21;ingress-zone=CUCM11

Call-ID: d58f2680-9c91200a-1c7ba-1501a8c0@192.168.1.21

CSeq: 101 INVITE

From: "Jonathan Robb"

;tag=505817~c9cc7ddc-9592-49e8-a13c-79e26f48eebc-30106972

To:

Server: TANDBERG/4135 (X8.10.2) Warning: 399 192.168.1.6:7003 "Policy Response"
Session-ID: 00000000000000000000000000000000;remote=75957d4fb66a13e835c10737aa505813 Content-
Length: 0

Ces données peuvent indiquer deux choses :

1. L'Expressway-E n'a jamais tenté d'envoyer une invitation (INVITE) à Cisco Webex
2. L'Expressway-E était la partie responsable de prendre la décision logique de refuser l'appel au moyen d'une erreur 404.

En général, l'erreur 04 Not Found signifie que l'Expressway n'est pas en mesure de trouver l'adresse de destination. Puisque les Expressways utilisent les règles de recherche pour acheminer les appels entre eux et entre différents environnements, commencez par axer vos efforts sur xConfiguration dans l'Expressway-E. Dans xConfiguration, vous pouvez consulter pour règle de recherche qui devrait transmettre l'appel à la zone DNS de Webex Hybrid. Pour trouver les règles de recherche configurées sur l'Expressway sous l'angle de xConfiguration, vous pouvez faire la recherche suivante « xConfiguration Zones Policy SearchRules Rule ». Par la suite, vous verrez apparaître une liste de configuration réunissant chacune des règles de recherche créées sur l'Expressway. Le nombre indiqué après la règle (« Rule ») augmentera en fonction de la règle de recherche qui a été créée en premier, qui porte le 1. Si vous avez de la difficulté à repérer la règle de recherche, vous pouvez utiliser les valeurs courantes de noms, comme « Webex » pour faciliter le repérage de la règle de recherche. Une autre manière d'identifier la règle consiste à rechercher la valeur de chaîne de modèle définie sur ".*@.*\ciscopark\.com". Il s'agit de la chaîne de caractères du schéma qui doit faire l'objet de la configuration. *(selon l'hypothèse voulant que la chaîne de caractères du schéma soit bien configurée)*Après la consultation de xConfiguration pour ce cas-ci, vous pourrez voir que la règle de recherche 6 est la règle appropriée pour transmettre l'appel à Cisco Webex.

```
*c xConfiguration Zones Policy SearchRules Rule 6 Authentication: "No"  
*c xConfiguration Zones Policy SearchRules Rule 6 Description: "Outbound calls to Webex"  
*c xConfiguration Zones Policy SearchRules Rule 6 Mode: "AliasPatternMatch"  
*c xConfiguration Zones Policy SearchRules Rule 6 Name: "Webex Hybrid - to Webex Cloud"  
*c xConfiguration Zones Policy SearchRules Rule 6 Pattern Behavior: "Leave"  
*c xConfiguration Zones Policy SearchRules Rule 6 Pattern Replace:  
*c xConfiguration Zones Policy SearchRules Rule 6 Pattern String: ".*@.*\ciscopark\.com"  
*c xConfiguration Zones Policy SearchRules Rule 6 Pattern Type: "Regex"  
*c xConfiguration Zones Policy SearchRules Rule 6 Priority: "101"  
*c xConfiguration Zones Policy SearchRules Rule 6 Progress: "Stop"  
*c xConfiguration Zones Policy SearchRules Rule 6 Protocol: "SIP"  
*c xConfiguration Zones Policy SearchRules Rule 6 SIPTrafficType: "Any"  
*c xConfiguration Zones Policy SearchRules Rule 6 Source Mode: "Named"  
*c xConfiguration Zones Policy SearchRules Rule 6 Source Name: "Hybrid Call Service Traversal"  
*c xConfiguration Zones Policy SearchRules Rule 6 State: "Enabled"  
*c xConfiguration Zones Policy SearchRules Rule 6 SystemGenerated: "No"  
*c xConfiguration Zones Policy SearchRules Rule 6 Target Name: "Hybrid Call Services DNS"  
*c xConfiguration Zones Policy SearchRules Rule 6 Target SIPVariant: "Any"  
*c xConfiguration Zones Policy SearchRules Rule 6 Target Type: "Zone"
```

Pour mettre à l'essai ce schéma, nous pouvons recourir à la fonction Check pattern (vérifier le schéma) qui est décrite dans le. Dans le cas présent, le message important tient à ce que nous voulons néanmoins que les valeurs suivantes soient configurées :Maintenance > Tools > Check pattern

- Alias : %Request URI in the initial INVITE% (Par exemple, pstojano-test@dmzlab.call.ciscopark.com)
- Pattern type (type de schéma) : Regex
- Chaîne de schéma .*@.*\ciscopark\.com

- Pattern behavior (comportement de schéma) : Congé

Si le Regex de la règle est configuré correctement, vous verrez le résultat positif de ce schéma. Ci-dessous, vous verrez une illustration de cette démarche, comme l'indique l'image :

Check pattern

Alias: pstojano-test@dmzlab.call.ciscopark.com

Pattern type: Regex

Pattern string: .*@.*.ciscopark.com

Pattern behavior: Leave

Result

Result: Succeeded

Details: Alias matched pattern

Alias: pstojano-test@dmzlab.call.ciscopark.com

Maintenant que vous pouvez confirmer que la règle de recherche est établie et qu'elle est configurée correctement, vous pouvez examiner de plus près la logique de recherche que l'Expressway applique pour déterminer si cela a des effets sur l'Expressway-E qui envoie l'erreur 404 Not Found. Voici un exemple de la logique de règle de recherche que l'Expressway met en application.

```

2017-09-25T11:26:02.966-04:00 amer-expressway01 tvcs: UTCTime="2017-09-25 15:26:02,966"
Module="network.search" Level="DEBUG": Detail="Search rule 'B2B calls to VCS-C' did not match
destination alias 'pstojano-test@dmzlab.call.ciscopark.com'"
2017-09-25T11:26:02.966-04:00 amer-expressway01 tvcs: UTCTime="2017-09-25 15:26:02,966"
Module="network.search" Level="DEBUG": Detail="Search rule 'Webex Hybrid' ignored due to source
filtering"
2017-09-25T11:26:02.966-04:00 amer-expressway01 tvcs: UTCTime="2017-09-25 15:26:02,966"
Module="network.search" Level="DEBUG": Detail="Search rule 'Calls to Webex' did not match
destination alias 'pstojano-test@dmzlab.call.ciscopark.com'"
2017-09-25T11:26:02.967-04:00 amer-expressway01 tvcs: UTCTime="2017-09-25 15:26:02,967"
Module="network.search" Level="DEBUG": Detail="Considering search rule 'to DNS' towards target
'DNS' at priority '100' with alias 'pstojano-test@dmzlab.call.ciscopark.com'"

2017-09-25T11:26:02.968-04:00 amer-expressway01 tvcs: UTCTime="2017-09-25 15:26:02,968"
Module="network.dns" Level="DEBUG": Detail="Sending DNS query" Name="dmzlab.call.ciscopark.com"
Type="NAPTR (IPv4 and IPv6)"
2017-09-25T11:26:02.982-04:00 amer-expressway01 tvcs: UTCTime="2017-09-25 15:26:02,982"
Module="network.dns" Level="DEBUG": Detail="Could not resolve hostname"
2017-09-25T11:26:02.982-04:00 amer-expressway01 tvcs: UTCTime="2017-09-25 15:26:02,982"
Module="network.dns" Level="DEBUG": Detail="Sending DNS query"
Name="_sips._tcp.dmzlab.call.ciscopark.com" Type="SRV (IPv4 and IPv6)"

```

Dans cet exemple, vous pouvez voir l'Expressway traiter quatre règles de recherche. Les trois premières n'ont pas été envisagées pour diverses raisons. Toutefois, la quatrième a été prise en compte. L'aspect intéressant de ces données est le suivant: immédiatement après son examen des règles, l'Expressway adopte la logique de recherche DNS. Si vous vous rappelez de ce que nous avons abordé plus tôt, dans xConfiguration, la règle de recherche configurée pour Webex Hybrid est nommée comme suit : Webex Hybrid - to Webex Cloud, et cette règle n'a même pas été envisagée dans la logique de règle de recherche ci-dessus. À ce stade-ci, il convient d'envisager comment la règle de recherche prise en compte (« to DNS ») a été mise en œuvre, afin que vous puissiez mieux comprendre si elle a des effets sur l'utilisation de la règle de recherche Webex Hybrid. Pour ce faire, vous pouvez revoir xConfig. Cette fois-ci, vérifiez si vous

repérez la règle de recherche qui s'appelle « to DNS »

```
*c xConfiguration Zones Policy SearchRules Rule 1 Authentication: "No"
*c xConfiguration Zones Policy SearchRules Rule 1 Description:
*c xConfiguration Zones Policy SearchRules Rule 1 Mode: "AliasPatternMatch"
*c xConfiguration Zones Policy SearchRules Rule 1 Name: "to DNS"
*c xConfiguration Zones Policy SearchRules Rule 1 Pattern Behavior: "Leave"
*c xConfiguration Zones Policy SearchRules Rule 1 Pattern Replace:
*c xConfiguration Zones Policy SearchRules Rule 1 Pattern String: "(?!.*@%localdomains%.*$).*"
*c xConfiguration Zones Policy SearchRules Rule 1 Pattern Type: "Regex"
*c xConfiguration Zones Policy SearchRules Rule 1 Priority: "100"
*c xConfiguration Zones Policy SearchRules Rule 1 Progress: "Stop"
*c xConfiguration Zones Policy SearchRules Rule 1 Protocol: "Any"
*c xConfiguration Zones Policy SearchRules Rule 1 SIPTrafficType: "Any"
*c xConfiguration Zones Policy SearchRules Rule 1 Source Mode: "Any"
*c xConfiguration Zones Policy SearchRules Rule 1 Source Name: "Please Select"
*c xConfiguration Zones Policy SearchRules Rule 1 State: "Enabled"
*c xConfiguration Zones Policy SearchRules Rule 1 SystemGenerated: "No"
*c xConfiguration Zones Policy SearchRules Rule 1 Target Name: "DNS"
*c xConfiguration Zones Policy SearchRules Rule 1 Target SIPVariant: "Any"
*c xConfiguration Zones Policy SearchRules Rule 1 Target Type: "Zone"
```

Après la révision de cette règle de recherche, vous pourrez tirer les conclusions suivantes :

- La chaîne de caractères du schéma correspondrait à l'URI de la demande de Cisco Webex
- La priorité est réglée à 100
- Les progrès (Progress, Pattern behavior) sont réglés à Arrêt (Stop).

Ces renseignements nous indiquent que l'URI de demande de Cisco Webex recevant l'appel pourrait correspondre à cette règle et que si la règle était mise en correspondance, l'Expressway cesserait de chercher (et d'envisager) d'autres règles de recherche. À la lumière de ces connaissances, l'ordre de priorité des règles devient un facteur clé. Dans l'Expressway, la priorité des règles de recherche fonctionne comme suit : la règle assortie du niveau de priorité le plus bas est tentée en premier. Voici un exemple ci-dessous. Search Rule (règle de recherche) :

MunicipalPattern behavior (comportement de schéma) : Continuer
Priorité 1 Search Rule (règle de recherche) : Neighbor (voisin)
Pattern behavior (comportement de schéma) : Continuer
Priorité 10 Search Rule (règle de recherche) : DNS
Pattern behavior (comportement de schéma) : Arrêter
Priorité 50 Dans cet exemple, la règle de recherche nommée Local (1) serait tentée en premier. Si une correspondance était révélée, le processus passerait à la règle de recherche voisine (10) compte tenu du comportement de schéma configuré pour continuer. Si la règle de recherche voisine ne faisait pas l'objet d'une correspondance, le processus continuerait néanmoins jusqu'à la règle de recherche DNS (50) qui serait considérée comme la dernière. Si la règle de recherche pour DNS a fait l'objet d'une correspondance, la recherche s'arrêtera, peu importe s'il y a une autre règle de recherche, dont la priorité dépasse 50, parce que le comportement de schéma est configuré pour arrêter. Compte tenu de ces connaissances, vous pouvez jeter un œil aux priorités des règles de recherche établies entre les règles « to DNS » et « Webex Hybrid - to Webex Cloud ».

```
*c xConfiguration Zones Policy SearchRules Rule 1 Name: "to DNS"
*c xConfiguration Zones Policy SearchRules Rule 1 Priority: "100"
*c xConfiguration Zones Policy SearchRules Rule 1 Progress: "Stop"

*c xConfiguration Zones Policy SearchRules Rule 6 Name: "Webex Hybrid - to Webex Cloud"
*c xConfiguration Zones Policy SearchRules Rule 6 Priority: "101"
*c xConfiguration Zones Policy SearchRules Rule 6 Progress: "Stop"
```

Ici, vous pouvez voir que la règle « to DNS » a une priorité inférieure à la règle « Webex Hybrid - to Webex Cloud » — par conséquent, la règle « to DNS » sera essayée en premier. Étant donné que le comportement de schéma (Progrès) est réglé pour l'arrêt, l'Expressway-E n'envisage jamais la règle Webex Hybrid - to Webex Cloud et l'appel échoue. Solution Ce type de problème est de plus en plus courant avec Hybrid Call Service Connect. Dans nombre de cas, au déploiement de la solution, les gens créent une règle assortie d'un haut niveau de priorité pour les

recherches Cisco Webex. Dans nombre de cas, la règle créée ne sera pas invoquée, car les règles existantes assorties d'un moindre niveau de priorité sont mises en correspondances, ce qui entraîne un échec. Ce problème se produit lors des appels entrants et sortants de Cisco Webex. Pour résoudre ce problème, vous devrez suivre ces étapes :

1. Ouvrez une session dans l'Expressway-E
2. Naviguez jusqu'à Configuration > Dial Plan > Search rules
3. Trouvez la règle de recherche Webex Hybrid et cliquez dessus (*Par ex. : Name : Webex Hybrid - to Webex Cloud*)
4. Définir la valeur de la priorité à un seuil inférieur aux autres règles de recherche; la valeur doit toutefois être assez élevée pour qu'il n'y ait pas d'incidence sur les autres. (*Par exemple, Priorité : 99*)

En règle générale, pour ce qui concerne les règles de recherche, plus les chaînes de mots des schémas sont précises, plus bas il est possible de les placer dans la liste de priorité des règles de recherche. Généralement, une zone DNS est configurée avec une chaîne de mots de schéma susceptibles de saisir tout ce qui n'est pas un domaine local et de l'envoyer à Internet. C'est pourquoi il est recommandé que vous définissez ce type de règle de recherche selon un niveau de priorité élevée, afin qu'elle soit invoquée en dernier lieu. Problème 4. Erreur de configuration CPL ExpresswayLa solution Expressway permet la mise en œuvre de mesures de protection de la fraude touchant les appels interurbains grâce à la logique de langage de traitement des appels (CPL). Si la solution d'Expressway en cours de déploiement sert seulement pour les accès mobiles et distants et Cisco Webex Hybrid Call Service, nous recommandons vivement que les règles et la politique de CPL soient activées et mises en œuvre. Alors que la configuration CPL sur l'Expressway pour Cisco Webex Hybrid est plutôt simple, une mauvaise configuration peut facilement bloquer des tentatives. Les scénarios ci-dessous montrent comment utiliser la journalisation de diagnostic pour repérer une erreur de configuration de CPL. Comme dans tous nos autres scénarios d'appels sortants acheminés, les symptômes demeurent identiques :

- L'application Cisco Webex de l'utilisateur appelé fait apparaître un bouton pour se joindre à l'appel (Join)
- Le téléphone qui fait l'appel émet une tonalité de rappel
- Le téléphone sur les lieux de l'utilisateur appelé sonne
- L'application de l'utilisateur appelé n'a jamais sonné

Comme dans tous les autres scénarios, vous pouvez utiliser des traces de SDL de CUCM, de même que des rapports de journalisation de diagnostic de l'Expressway-C et de l'Expressway-E. Comme précédemment, vous devez faire référence à la pour utiliser l'historique de recherche et des conseils pour identifier un appel dans les journaux de diagnostic. De nouveau, au moyen de l'historique de recherche de l'Expressway-E, il est déterminé que l'appel était en train d'arriver lorsqu'il a défailli. Vous trouverez ci-dessous le début de l'analyse permettant d'examiner l'invitation de SIP arrivant dans l'Expressway-E en provenance de l'Expressway-C.

```
2017-09-25T16:54:43.722-04:00 amer-expressway01 tvcs: UTCTime="2017-09-25 20:54:43,722"
Module="network.sip" Level="DEBUG": Action="Received" Local-ip="192.168.1.6" Local-port="7003"
Src-ip="192.168.1.5" Src-port="26404" Msg-Hash="17204952472509519266"
SIPMSG:
|INVITE sip:pstojano-test@dmzlab.call.ciscospark.com SIP/2.0
Via: SIP/2.0/TLS 192.168.1.5:5061;egress-
zone=HybridCallServiceTraversal;branch=z9hG4bK781a130d234ed9aaec86834368739430283256.34216c32a0d
e36e16590bae36df388b6;proxy-call-id=3bbbf94a-082e-4088-8f5a-5ea7e82f8aac;rport
Via: SIP/2.0/TCP 192.168.1.21:5065;branch=z9hG4bK1cf344a8b117e;received=192.168.1.21;ingress-
zone=CUCM11
Call-ID: c030f100-9c916d13-1cdcb-1501a8c0@192.168.1.21
CSeq: 101 INVITE
Call-Info: <urn:x-cisco-remotecallinfo>;x-cisco-video-traffic-class=DESKTOP
Remote-Party-ID: "Jonathan Robb"
<sip:5010@rtp.ciscotac.net>;party=calling;screen=yes;privacy=off
Contact: <sip:5010@192.168.1.21:5065;transport=tcp>;video;audio
```

From: "Jonathan Robb"

;tag=512579~c9cc7ddc-9592-49e8-a13c-79e26f48eebc-30107000

To:

Max-Forwards: 15

Record-Route: <sip:proxy-call-id=3bbbf94a-082e-4088-8f5a-5ea7e82f8aac@192.168.1.5:5061;transport=tls;lr>

Record-Route: <sip:proxy-call-id=3bbbf94a-082e-4088-8f5a-5ea7e82f8aac@192.168.1.5:5060;transport=tcp;lr>

Allow: INVITE, OPTIONS, INFO, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE, NOTIFY

User-Agent: Cisco-CUCM11.5

Expires: 180

Date: Mon, 25 Sep 2017 20:54:43 GMT

Supported: timer, resource-priority, replaces, X-cisco-srtp-fallback, X-cisco-original-called

Session-Expires: 1800

Min-SE: 1800

Allow-Events: presence

X-TAATag: 4ffffefed-0512-4067-ac8c-35828f0a1150

Session-ID: 75957d4fb66a13e835c10737aa512577;remote=00000000000000000000000000000000

Cisco-Guid: 3224432896-0000065536-0000000264-0352430272

Content-Type: application/sdp

Content-Length: 714

<SDP Omitted>

Grâce à l'ID de l'appel (Call-ID c030f100-9c916d13-1cdcb-1501a8c0) dans l'en-tête de SIP, vous pouvez effectuer rapidement une recherche dans l'ensemble des messages associés à ce dialogue. Lorsque vous consultez la troisième occurrence dans les journaux pour ce Call-ID, vous pouvez voir que l'Expressway-E envoie immédiatement une erreur 403 Forbidden à l'Expressway-C.

2017-09-25T16:54:43.727-04:00 amer-expressway01 tvcs: UTCTime="2017-09-25 20:54:43,727"

Module="network.sip" Level="DEBUG": Action="Sent" Local-ip="192.168.1.6" Local-port="7003" Dst-ip="192.168.1.5" Dst-port="26404" Msg-Hash="9195436101110134622"

SIPMSG:

|SIP/2.0 403 Forbidden

Via: SIP/2.0/TLS 192.168.1.5:5061;egress-

zone=HybridCallServiceTraversal;branch=z9hG4bK781a130d234ed9aaec86834368739430283256.34216c32a0de36e16590bae36df388b6;proxy-call-id=3bbbf94a-082e-4088-8f5a-

5ea7e82f8aac;received=192.168.1.5;rport=26404;ingress-zone=HybridCallServiceTraversal

Via: SIP/2.0/TCP 192.168.1.21:5065;branch=z9hG4bK1cf344a8b117e;received=192.168.1.21;ingress-zone=CUCM11

Call-ID: c030f100-9c916d13-1cdcb-1501a8c0@192.168.1.21

CSeq: 101 INVITE

From: "Jonathan Robb"

;tag=512579~c9cc7ddc-9592-49e8-a13c-79e26f48eebc-30107000

To:

;tag=64fe7f9eab37029d

Server: TANDBERG/4135 (X8.10.2)

Warning: 399 192.168.1.6:7003 "Policy Response"
Session-ID: 00000000000000000000000000000000;remote=75957d4fb66a13e835c10737aa512577
Content-Length: 0

Pour connaître les motifs pour lesquels l'Expressway-E a refusé cet appel et envoyé une erreur 403 à l'Expressway-C, vous voudrez analyser les entrées de journal entre l'erreur Forbidden 403 et l'invitation originale de SIP (SIP INVITE) qui est arrivée dans l'Expressway. Une analyse des entrées du journal permet généralement de voir toutes les décisions logiques qui sont prises. À noter que vous ne verrez pas de règles de recherche invoquées, mais que vous repérerez une logique de CPL en cours. Voici un extrait illustrant ces entrées.

```
2017-09-25T16:54:43.725-04:00 amer-expressway01 tvcs: UTCTime="2017-09-25 20:54:43,725"  
Module="network.cpl" Level="DEBUG": Remote-ip="192.168.1.5" Remote-port="26404" Detail="CPL:
```

```
2017-09-25T16:54:43.725-04:00 amer-expressway01 tvcs: UTCTime="2017-09-25 20:54:43,725"  
Module="network.cpl" Level="DEBUG": Remote-ip="192.168.1.5" Remote-port="26404" Detail="CPL:
```

```
2017-09-25T16:54:43.725-04:00 amer-expressway01 tvcs: UTCTime="2017-09-25 20:54:43,726"  
Module="network.cpl" Level="DEBUG": Remote-ip="192.168.1.5" Remote-port="26404" Detail="CPL:
```

```
2017-09-25T16:54:43.725-04:00 amer-expressway01 tvcs: UTCTime="2017-09-25 20:54:43,726"  
Module="network.cpl" Level="DEBUG": Remote-ip="192.168.1.5" Remote-port="26404" Detail="CPL:
```

En fonction de l'analyse de journal présentée ci-dessus, vous pouvez effectuer la détermination que la CPL rejette l'appel.

```
2017-09-25T16:54:43.725-04:00 amer-expressway01 tvcs: Event="Search Completed"  
Reason="Forbidden" Service="SIP" Src-alias-type="SIP" Src-alias="5010@rtp.ciscotac.net" Dst-alias-type="SIP" Dst-alias="sip:pstojano-test@dmzlab.call.ciscospark.com" Call-serial-number="48c80582-ec79-4d89-82e2-e5546f35703c" Tag="4ffefed-0512-4067-ac8c-35828f0a1150" Detail="found:false, searchtype:INVITE, Info:Policy Response" Level="1" UTCTime="2017-09-25 20:54:43,726"
```

```
2017-09-25T16:54:43.725-04:00 amer-expressway01 tvcs: Event="Call Rejected" Service="SIP" Src-ip="192.168.1.5" Src-port="26404" Src-alias-type="SIP"
```

Note: Dans cette situation, vous ne voyez pas de règles de recherche invoquées, car les fonctions CPL, FindMe et Transforms sont toutes traitées avant une règle de recherche. Dans la plupart des cas, vous pouvez utiliser xConfig de l'Expressway pour mieux comprendre les circonstances. Toutefois, pour CPL, vous ne pouvez pas voir les règles définies. Tout ce que vous pouvez voir, c'est si la politique a été activée. Voici la partie de xConfig indiquant que l'Expressway-E fait appel à la logique de CPL locale.

```
*c xConfiguration Policy AdministratorPolicy Mode: "LocalCPL"
```

Pour mieux comprendre la configuration de la règle, vous devez ouvrir une session dans l'Expressway-E et naviguer jusqu'à Configuration > Call Policy > Rules, comme l'indique l'image.

Source	Destination	Action	Reorder
☐	*@dmzlab.call.ciscospark.com	Reject	↓

En examinant cette configuration, vous pourrez voir que les éléments suivants sont

configurés Source : .* Destination : .*@dmzlab\call.ciscospark\com.* Action : Rejeter Comparativement à ce qui est indiqué dans le [guide de déploiement de Cisco Webex Hybrid Call Service](#), vous pouvez voir que la source et la destination ont été configurées à l'envers.

Field	Setting
Source Type	From address
Rule applies to	Unauthenticated callers
Source pattern	.*@example\call.ciscospark\com.*, where example is your company's subdomain.
Destination pattern	.*
Action	Reject

Solution Pour résoudre ce problème, vous devez réajuster la configuration de la règle CPL de sorte que la source soit définie sur .*@%Webex_subdomain%\call.ciscospark\com.* et le modèle de destination est .*

1. Ouvrez une session dans l'Expressway-E
2. Naviguez jusqu'à Configuration > Call Policy > Rules
3. Sélectionnez la règle configurée pour le service Cisco Webex Hybrid Call
4. Entrez le modèle source comme .*@%Webex_subdomain%\call.ciscospark\com.*(Ex : .*@dmzlab\call.ciscospark\com.*)
5. Entrez le modèle de destination .*
6. Sélectionnez Save (enregistrer)

Pour en savoir plus sur la mise en œuvre de CPL pour Webex Hybrid, consultez le [guide de destination Cisco Webex Hybrid](#). Bidirectionnel : Cisco Webex vers le site ou le site vers Cisco Webex Problème 1. Le téléphone IP/terminal de collaboration offre un codec audio autre que G.711, G.722 ou AAC-LD. Hybrid Call Service Connect prend en charge trois codecs audio différents : G.711, G.722 et AAC-LD. Pour parvenir à établir un appel avec l'environnement de Cisco Webex, il faut utiliser l'un des codecs audio. L'environnement sur les lieux peut être configuré pour plusieurs types de codecs audios. Tout à la fois, la configuration peut viser à en limiter l'utilisation. Cela peut arriver délibérément ou par accident, lors de l'utilisation de paramètres sur mesure ou de paramètres régionaux établis par défaut dans Unified CM. Pour ce comportement en particulier, les schémas de journalisation peuvent varier en fonction de la direction de l'appel et de la question de savoir si Unified CM a été configuré pour utiliser l'offre rapide ou retardée (Early ou Delayed). Voici des exemples de quelques situations dans lesquelles ce comportement pourrait se présenter spontanément :

1. Cisco Webex envoie une intitaon entrante avec SDP qui offre G.711, G.722 ou AAC-LD. L'Expressway-C envoie ce message à Unified CM, mais Unified CM est configuré pour ne permettre que G.729 pour cet appel. Ainsi, Unified CM refusera l'appel faute de codec disponible.
2. Unified CM tente l'appel sortant *sous forme d'offre rapide vers Cisco Webex, ce qui signifie que l'invitation initiale envoyée à l'Expressway-C contiendra le SDP QUI PREND EN CHARGE SEULEMENT l'audio G.729*. Cisco Webex envoie ensuite un 200 OK avec SDP qui déconnecte l'audio (*m=audio 0 RTP/SAVP*), car il ne prend pas en charge G.729. Une fois que l'Expressway-C transmet l'invitation (INVITE) à Unified CM, Unified CM met fin à l'appel faute de codec disponible.
3. Unified CM tente l'appel sortant *sous forme d'offre retardée vers Cisco Webex, ce qui signifie que l'invitation initiale envoyée à l'Expressway-C ne contiendra pas de SDP*. Cisco Webex

envoi ensuite un 200 OK avec SDP qui contient tous les codecs pris en charge par Cisco Webex. L'Expressway-C envoie ce 200 OK à Unified CM, mais Unified CM est configuré pour ne permettre que G.729 pour cet appel. Ainsi, Unified CM refusera l'appel faute de codec disponible.

Si vous tentez de cerner un échec d'appel d'Hybrid Call Service Connect qui correspond à ce problème, vous devez obtenir les journaux d'Expressway en plus des traces de SDL d'Unified CM. Les extraits de journaux ci-dessous présentent la situation 2 dans laquelle Unified CM tente de faire l'appel sortant en tant qu' *offre rapide*. Parce que nous savons que l'appel provient de Cisco Webex, l'analyse de journal débute sur l'Expressway-E. Voici un extrait de l'invitation initiale envoyée à Cisco Webex. Vous pouvez voir que le codec audio préféré est réglé à G.729 (charge utile 18). Le 101 est pour DTMF. Dans ce scénario en particulier, ce n'est pas pertinent.

```
2017-09-19T10:46:10.488-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 14:46:10,488"
Module="network.sip" Level="DEBUG": Action="Sent" Local-ip="172.16.2.2" Local-port="25034" Dst-
ip="146.20.193.64" Dst-port="5062" Msg-Hash="4309505007645007056"
SIPMSG:
INVITE sip:pstojano-test@dmzlab.call.ciscospark.com SIP/2.0
Via: SIP/2.0/TLS 64.102.241.236:5062;egress-
zone=HybridCallServicesDNS;branch=z9hG4bK323e6b15ad0cbbf409751f67848136fa1115;proxy-call-
id=a3a78ee2-c01b-4741-b29b-55aede256d2;rport
Via: SIP/2.0/TLS 172.16.2.2:5073;branch=z9hG4bK350703fe46645f0acddef05b35adc5c157;x-cisco-local-
service=nettle;received=172.16.2.2;rport=41511;ingress-zone=DefaultZone
Via: SIP/2.0/TLS 192.168.1.6:5061;egress-
zone=DefaultZone;branch=z9hG4bKf71f2bf47233d6ca52b579364594ac6c1114.a402e3f25603f5a77b60b17ea47d
bf72;proxy-call-id=be17a470-0bca-4ad5-8a6c-14872e007efb;received=192.168.1.6;rport=25025
Via: SIP/2.0/TLS 192.168.1.5:5061;egress-
zone=HybridCallServiceTraversal;branch=z9hG4bKf4cf4cf09d213a88bd2331cef0bc82b540559.494a140082bd
66357134b9eed4335df8;proxy-call-id=d4d4e950-babc-45d5-a4a7-
c60a8b17a8bd;received=192.168.1.5;rport=26513;ingress-zone=HybridCallServiceTraversal
Via: SIP/2.0/TCP 192.168.1.21:5065;branch=z9hG4bK12dd82194c4f7;received=192.168.1.21;ingress-
zone=CUCM11
Call-ID: 44bdd400-9c112db1-12d95-1501a8c0@192.168.1.21
CSeq: 101 INVITE
Remote-Party-ID: "Jonathan Robb" <sip:5010@rtp.ciscotac.net>;privacy=off;screen=no;party=calling
Contact: <sip:172.16.2.2:5073;transport=tls>;video;audio
From: "Jonathan Robb"
```

```
Max-Forwards: 14
Record-Route: <sip:proxy-call-id=a3a78ee2-c01b-4741-b29b-
55aede256d2@64.102.241.236:5062;transport=tls;lr>
Record-Route: <sip:proxy-call-id=a3a78ee2-c01b-4741-b29b-
55aede256d2@172.16.2.2:5061;transport=tls;lr>
Allow: INVITE,ACK,BYE,CANCEL,INFO,OPTIONS,REFER,SUBSCRIBE,NOTIFY
User-Agent: TANDBERG/4352 (X8.10.2-b2bua-1.0)
Supported: X-cisco-srtp-fallback,replaces,timer
Session-Expires: 1800;refresher=uac
Min-SE: 500
X-TAATag: 14a0bd87-1825-4ecf-9f3d-4a23cfa69725
Session-ID: 75957d4fb66a13e835c10737aa329445;remote=00000000000000000000000000000000
Content-Type: application/sdp
Content-Length: 1407
```

```
v=0
o=tandberg 0 1 IN IP4 64.102.241.236
s=-
c=IN IP4 64.102.241.236
b=AS:384
t=0 0
```

```
m=audio 52668 RTP/SAVP 18 101 <-- CUCM is only supporting G.729 for this call
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=no
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:.....
a=crypto:2 AES_CM_128_HMAC_SHA1_80 inline:.....
UNENCRYPTED_SRTCP
a=crypto:3 AES_CM_128_HMAC_SHA1_32 inline:.....
a=crypto:4 AES_CM_128_HMAC_SHA1_32 inline:.....
UNENCRYPTED_SRTCP
a=sendrecv
a=rtcp:52669 IN IP4 64.102.241.236
m=video 52670 RTP/SAVP 126 97
b=TIAS:384000
a=rtpmap:126 H264/90000
a=fmtp:126 profile-level-id=42801e;packetization-mode=1;level-asymmetry-allowed=1
a=rtpmap:97 H264/90000
a=fmtp:97 profile-level-id=42801e;packetization-mode=0;level-asymmetry-allowed=1
a=rtcp-fb:* nack pli
a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:.....
a=crypto:2 AES_CM_128_HMAC_SHA1_80 inline:.....
UNENCRYPTED_SRTCP
a=crypto:3 AES_CM_128_HMAC_SHA1_32 inline:.....
a=crypto:4 AES_CM_128_HMAC_SHA1_32 inline:.....
UNENCRYPTED_SRTCP
a=sendrecv
a=content:main
a=label:11
a=rtcp:52671 IN IP4 64.102.241.236
```

En réponse à l'invitation initiale, Cisco Webex répond avec un message 200 OK. Si vous jetez un œil plus attentif à ce message, vous pouvez voir que le codec audio a été remis à zéro. Il s'agit d'un problème, car sans port audio attribué, l'appel ne sera pas en mesure de négocier ce flux.

```
2017-09-19T10:46:27.073-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 14:46:27,072"
Module="network.sip" Level="DEBUG": Action="Received" Local-ip="172.16.2.2" Local-port="25034"
Src-ip="146.20.193.64" Src-port="5062" Msg-Hash="5236578200712291002"
```

SIPMSG:

SIP/2.0 200 OK

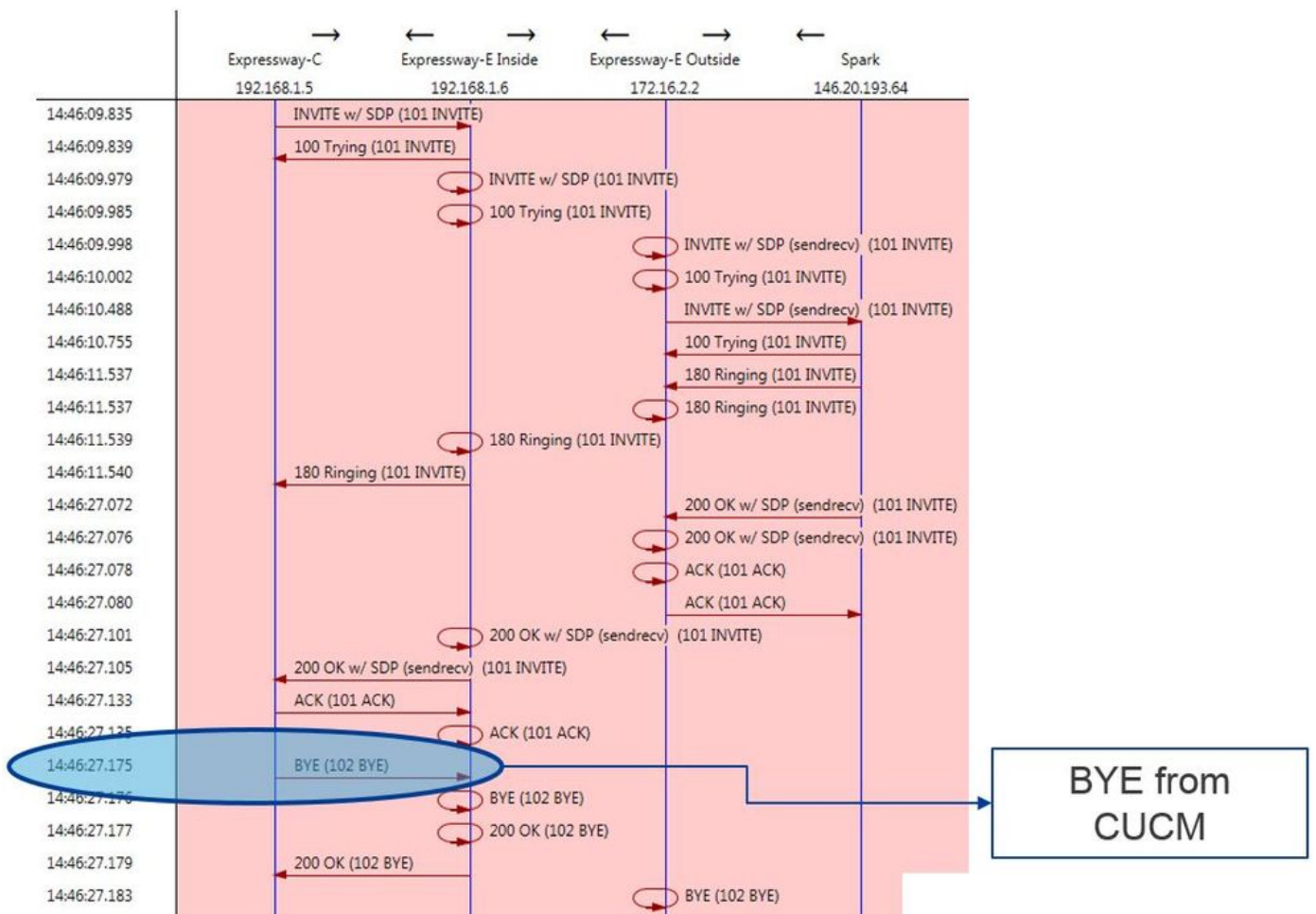
```
Via: SIP/2.0/TLS 64.102.241.236:5062;egress-
zone=HybridCallServicesDNS;branch=z9hG4bK323e6b15ad0cbbf409751f67848136fa1115;proxy-call-
id=a3a78ee2-c01b-4741-b29b-55aede256d2;rport=38245;received=192.168.5.26,SIP/2.0/TLS
172.16.2.2:5073;branch=z9hG4bK350703fe46645f0acdde05b35adc5c157;x-cisco-local-
service=nettle;received=172.16.2.2;rport=41511;ingress-zone=DefaultZone,SIP/2.0/TLS
192.168.1.6:5061;egress-
zone=DefaultZone;branch=z9hG4bKf71f2bf47233d6ca52b579364594ac6c1114.a402e3f25603f5a77b60b17ea47d
bf72;proxy-call-id=be17a470-0bca-4ad5-8a6c-
14872e007efb;received=192.168.1.6;rport=25025,SIP/2.0/TLS 192.168.1.5:5061;egress-
zone=HybridCallServiceTraversal;branch=z9hG4bKf4cfd09d213a88bd2331cef0bc82b540559.494a140082bd
66357134b9eed4335df8;proxy-call-id=d4d4e950-babc-45d5-a4a7-
c60a8b17a8bd;received=192.168.1.5;rport=26513;ingress-
zone=HybridCallServiceTraversal,SIP/2.0/TCP
192.168.1.21:5065;branch=z9hG4bK12dd82194c4f7;received=192.168.1.21;ingress-zone=CUCM11
Call-ID: 44bdd400-9c112db1-12d95-1501a8c0@192.168.1.21
CSeq: 101 INVITE
Contact: "l2sip-UA" <sip:l2sip-UA@l2sip-cfa-01.wbx2.com:5062;transport=tls>
From: "Jonathan Robb"
```

```
Record-Route: <sip:l2sip-cfa-01.wbx2.com:5062;transport=tls;lr>,<sip:proxy-call-id=a3a78ee2-
c01b-4741-b29b-55aede256d2@64.102.241.236:5062;transport=tls;lr>,<sip:proxy-call-id=a3a78ee2-
```

c01b-4741-b29b-55aede256d2@172.16.2.2:5061;transport=tls;lr>
Allow: INVITE,ACK,CANCEL,BYE,REFER,INFO,OPTIONS,NOTIFY,SUBSCRIBE
User-Agent: Cisco-L2SIP
Supported: replaces
Accept: application/sdp
Allow-Events: kpml
Session-ID: ed35426ed3ade6fdc3b058792333df2b;remote=75957d4fb66a13e835c10737aa329445
Locus: 4711a33f-9d49-11e7-9bf6-dea12d0f2127
Locus-Type: CALL
Content-Type: application/sdp
Content-Length: 503

v=0
o=linus 0 1 IN IP4 146.20.193.109
s=-
c=IN IP4 146.20.193.109
b=TIAS:384000
t=0 0
m=audio 0 RTP/SAVP * <-- Webex is zeroing this port out
m=video 33512 RTP/SAVP 108
c=IN IP4 146.20.193.109
b=TIAS:384000
a=content:main
a=sendrecv
a=rtpmap:108 H264/90000
a=fmtp:108 profile-level-id=42001E;packetization-mode=1;max-mps=40500;max-fs=1620;max-fps=3000;max-br=10000;max-dpb=3037;level-asymmetry-allowed=1
a=rtcp-fb:* nack pli
a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:.....
a=label:200

Vous pouvez maintenant utiliser TranslatorX pour passer en revue le reste du dialogue. Vous constaterez que le dialogue s'achève avec un ACK. Le problème est immédiatement après la fin du dialogue il ya un BYE qui vient de la direction de l'Expressway-C comme indiqué dans l'image.



Voici un exemple détaillé du message BYE. Vous verrez que l'User-Agent (utilisateur-agent) est Cisco-CUCM11.5, ce qui signifie que le message a été généré par Unified CM. Un autre aspect à signaler : le code de motif s'établit à cause=47. La traduction courantes pour cette situation est No resource available (aucune ressource disponibles).

```

2017-09-19T10:46:27.175-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 14:46:27,175"
Module="network.sip" Level="DEBUG": Action="Received" Local-ip="192.168.1.6" Local-port="7003"
Src-ip="192.168.1.5" Src-port="26513" Msg-Hash="237943800593485079"
SIPMSG:
BYE sip:192.168.1.6:5071;transport=tls SIP/2.0
Via: SIP/2.0/TLS 192.168.1.5:5061;egress-
zone=HybridCallServiceTraversal;branch=z9hG4bK90a666b3461356f8cd605cec91e4538240575.494a140082bd
66357134b9eed4335df8;proxy-call-id=d4d4e950-babc-45d5-a4a7-c60a8b17a8bd;rport
Via: SIP/2.0/TCP 192.168.1.21:5065;branch=z9hG4bK12ddd10269d39;received=192.168.1.21;ingress-
zone=CUCM11
Call-ID: 44bdd400-9c112db1-12d95-1501a8c0@192.168.1.21
CSeq: 102 BYE
From: "Jonathan Robb" <sip:5010@rtp.ciscotac.net>;tag=329447~c9cc7ddc-9592-49e8-a13c-
79e26f48eebc-30106833
To: <sip:pstojano-test@dmzlab.call.ciscopark.com>;tag=f3734601fb0eb541
Max-Forwards: 69
Route: <sip:proxy-call-id=be17a470-0bca-4ad5-8a6c-
14872e007efb@192.168.1.6:7003;transport=tls;lr>, <sip:proxy-call-id=be17a470-0bca-4ad5-8a6c-
14872e007efb@192.168.1.6:5061;transport=tls;lr>
User-Agent: Cisco-CUCM11.5
Date: Tue, 19 Sep 2017 14:46:09 GMT
X-TAATag: 14a0bd87-1825-4ecf-9f3d-4a23cfa69725
Reason: Q.850 ;cause=47
Session-ID: 75957d4fb66a13e835c10737aa329445;remote=ed35426ed3ade6fdc3b058792333df2b
Content-Length: 0

```

Étant donné que Cisco Webex a réinitialisé le codec audio pour cet échantillon d'appel, nous allons axer nos efforts sur: a. l'invitation initiale qui a été envoyée à Cisco Webex et b. sur la logique que Cisco Webex a utilisée pour remettre ce port à zéro. Maintenant, en examinant ce qui

distingue l'invitation, nous pouvons observer qu'elle contient seulement G.729. Compte tenu de cela, passez en revue le guide de déploiement de Cisco Webex Hybrid Call Service et plus précisément, consultez le chapitre sur la préparation de votre environnement, dans lequel l'étape 5 de section sur la façon de [Satisfaire aux conditions requises pour Hybrid Call ServiceConnect précise les codecs qui sont pris en charge](#). Cela vous permettra de voir ceci :Cisco Webex prend en charge les codecs suivants :

- Audio : G.711, G.722, AAC-LD
- Vidéo — H.264

Note: Opus n'est pas utilisé sur le tronçon sur site de l'appel pour Cisco Webex Hybrid Call. Compte tenu de ces renseignements, vous pouvez conclure qu'Unified CM envoie un codec audio non pris en charge. C'est la raison pour laquelle Cisco Webex remet le port à zéro. Solution :Pour faire face à cette situation particulière, vous devrez peut-être examiner la configuration de la région entre Cisco Webex RD qui ancre l'appel sur site et la ligne principale SIP de l'Expressway-C. Pour ce faire, déterminez dans quel pool de périphériques se trouvent ces deux éléments. Le regroupement de périphériques contient les mises en correspondance avec les régions. Pour déterminer le regroupement de périphériques de la ligne principale SIP de l'Expressway-C :

1. Connectez-vous à Unified CM.
2. Accédez à Device > Trunk.
3. Recherchez le nom de liaison ou cliquez sur Rechercher.
4. Sélectionnez la ligne principale Expressway-C.
5. Enregistrez le nom du pool de périphériques.

Pour déterminer le pool de périphériques de CTI-RD ou de Cisco Webex-RD qui a relié l'appel :

1. Accédez à Device > Phone.
2. Lors de la recherche, vous pouvez sélectionner Device Type (Type de périphérique) contient Webex ou CTI Remote Device (Périphérique distant CTI) (selon ce que le client utilise).
3. Enregistrez le nom du pool de périphériques.

Déterminez la région associée à chaque pool de périphériques :

1. Accédez à System > Device Pool.
2. Faites une recherche pour trouver le regroupement de périphériques qui a servi pour la ligne principale de SIP sur l'Expressway-C.
3. Cliquez sur le pool de périphériques.
4. Enregistrez le nom de la région.
5. Faites une recherche pour trouver le regroupement de périphériques ayant servi pour Webex-RD ou CTI-RD.
6. Cliquez sur le pool de périphériques.
7. Enregistrez le nom de la région.

Déterminer la relation de la région :

1. Accédez à Système > Informations sur la région > Région.
2. Effectuez une recherche sur l'une des régions identifiées.
3. Déterminez s'il existe une relation Région entre les deux régions qui utilisent G.729.

À ce stade-ci, si vous repérez la relation qui utilise G.729, vous aurez besoin de préciser la relation pour prendre en charge les codecs audio pris en charge que Cisco Webex utilise ou encore, il faudra utiliser un autre regroupement de périphériques subordonné à une région qui le prend en charge. Dans le cas décrit ci-dessus, voici ce qui a été déterminé :Expressway-C Trunk Region (région de la ligne principale d'Expressway-C) : ReservingBandwidthWebex-RD Region (région de Webex-RD) : Périphériques de RTPVoici une illustration graphique de la relation entre les régions RTP-Devices et ReservingBandwidth, comme le montre l'image.

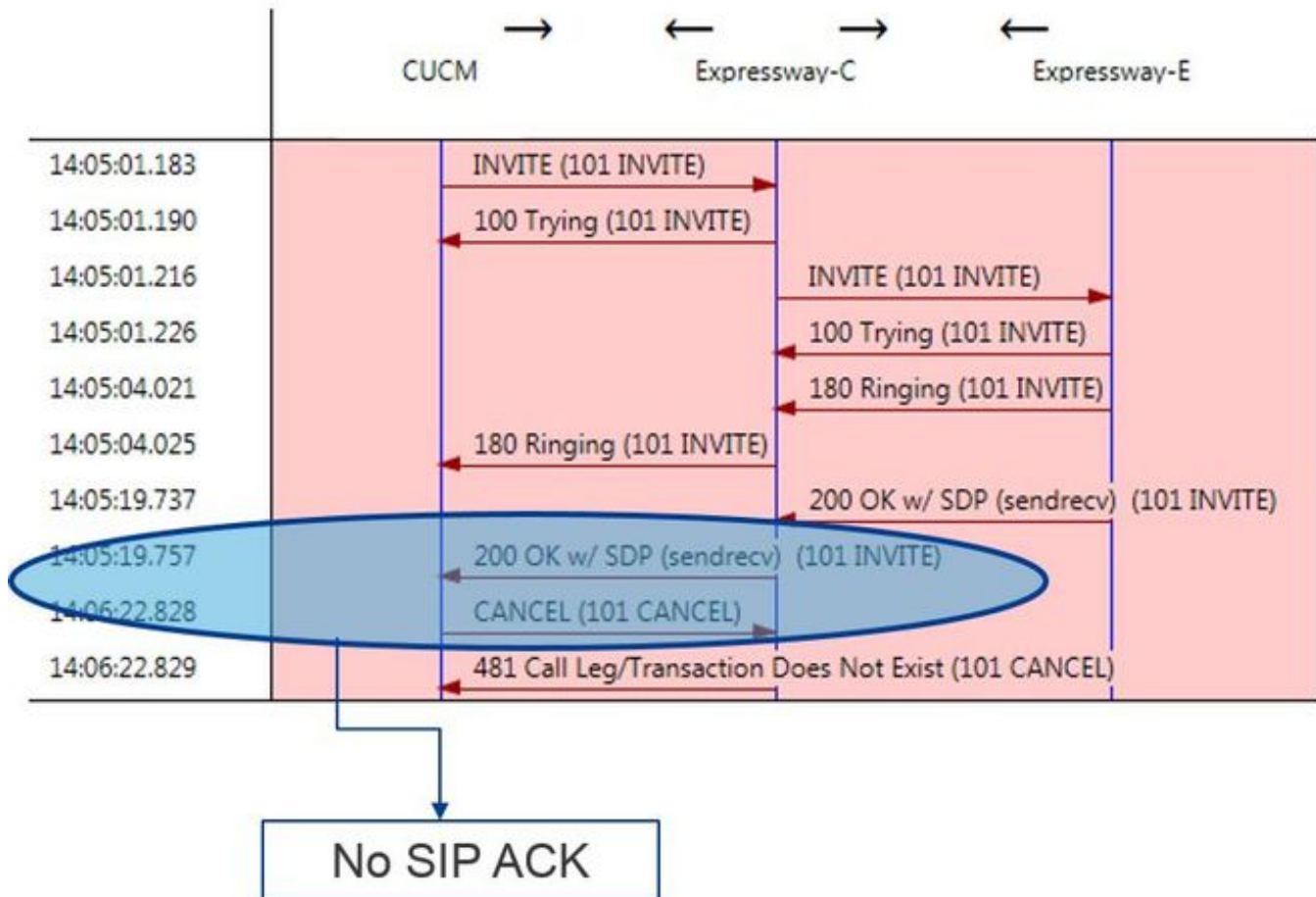
Region Information				
Name: RTP-Devices				
Region Relationships				
Region	Audio Codec Preference List	Maximum Audio Bit Rate	Maximum Session Bit Rate for Video Calls	Maximum Session Bit Rate for Immersive Video Calls
Default	Use System Default (Factory Default low loss)	256 kbps (L16, AAC-LD)	32000 kbps	32000 kbps
ReservingBandwidth	Use System Default (Factory Default low loss)	8 kbps (G.729)	384 kbps	384 kbps
RTP-Devices	Use System Default (Factory Default low loss)	256 kbps (L16, AAC-LD)	32000 kbps	32000 kbps
RTP-Infrastructure	Use System Default (Factory Default low loss)	256 kbps (L16, AAC-LD)	32000 kbps	32000 kbps

G.729 Not Supported by Spark

En modifiant le regroupement de périphériques dans lequel se trouvait la ligne principale d'Expressway-C, vous changez la relation sur le plan de la région. Le nouveau regroupement de périphériques a une région réglée à RTP-Infrastructure. Par conséquent, la nouvelle relation de région entre Cisco Webex-RD et la ligne principale d'Expressway-C s'est établie pour RTP-Devices et RTP-Infrastructure. Comme illustré, vous pouvez voir que cette relation prend en charge AAC-LD, qui est l'un des codecs audio pris en charge par Cisco Webex et que l'appel sera configuré correctement. Problème 2. Taille maximale du message entrant Unified CM dépassée Parce que la vidéo est de plus en plus répandue au sein de l'entreprise, la taille de messages SIP qui contiennent SDP s'est grandement accrue. Les serveurs qui traitent ces messages doivent être configurés de manière à accepter un paquet volumineux. Dans plusieurs serveurs de contrôle d'appel, les valeurs par défaut sont correctes. Avec les solutions Cisco Unified Communications Manager (Unified CM), les valeurs par défaut pour gérer un grand message SIP contenant SDP dans les versions derniers ont été pas. Dans les versions ultérieures d'Unified CM, la taille de valeur autorisée pour un message SIP a été augmentée. Cependant, cette valeur n'est définie que sur les nouvelles installations et non sur les mises à niveau. Ceci dit, les clients qui mettent à niveau leurs anciennes versions d'Unified CM pour prendre en charge Hybrid Call Service Connect peuvent être affectés par le fait que la taille maximale des messages entrants sur Unified CM est trop faible. Si vous tentez de cerner un échec d'appel d'Hybrid Call Service Connect qui correspond à ce problème, vous devez obtenir les journaux d'Expressway en plus des traces de SDL d'Unified CM. Afin d'identifier l'échec, commencez par comprendre ce qui se passe, puis les types de scénarios dans lesquels l'échec peut se produire. Pour répondre à la question de savoir ce qui se passe, vous devez savoir qu'une fois que Unified CM reçoit un message SIP trop volumineux, il ferme simplement le socket TCP et ne répond pas à l'Expressway-C. Cela dit, il y a plusieurs situations dans lesquelles cela peut se produire et plusieurs façon dont ça peut arriver :

1. Cisco Webex envoie une invitation (INVITE) avec SDP et elle est trop volumineuse. L'Expressway-C la transmet à Unified CM et Unified CM ferme le TCP Socket, ce qui interrompt le dialogue SIP.
2. Unified CM tente l'appel sortant sous forme d'offre rapide vers Webex, ce qui signifie que l'invitation initiale envoyée à l'Expressway-C contiendra le SDP. Cisco Webex envoie ensuite un 200 OK avec SDP en guise de réponse. La réponse 200 OK lorsqu'elle est transmise de l'Expressway-C à Unified CM, est trop volumineuse. Unified CM ferme le TCP Socket, puis le dialogue de SIP s'interrompt.
3. Unified CM tente l'appel sortant sous forme d'offre retardée vers Cisco Webex, ce qui signifie que l'invitation initiale envoyée à l'Expressway-C ne contiendra pas de SDP. Cisco Webex envoie ensuite un 200 OK avec SDP. L'offre de 200 OK, lorsqu'elle est transmise de l'Expressway-C à Unified CM, est trop volumineuse. Unified CM ferme le TCP Socket, puis le dialogue de SIP s'interrompt.

Des recherches dans les journaux d'Expressway-C pour cette condition en particulier vous aident à comprendre le flux du message. Si vous utilisez un programme comme [TranslatorX](#), vous pouvez voir que l'Expressway-C transmet le Cisco Webex 200 OK avec SDP à Unified CM. Le défi est le suivant : Unified CM ne répond jamais avec un ACK de SIP, comme le montre l'image.



Puisque Unified CM est la partie responsable de la non-réponse, il est utile de passer en revue les traces SDL pour voir comment Unified CM aborde cette situation. Dans ce scénario, Unified CM ignore le grand message de l'Expressway-C. Un élément de ligne comme celui-ci sera imprimé.

CUCM Traces

```
53138762.000 |09:05:19.762 |AppInfo |SIPSocketProtocol(5,100,14,707326)::handleReadComplete
send SdlReadRsp: size 5000
53138763.000 |09:05:19.762 |SdlSig |SdlReadRsp |wait
|SIPTcp(5,100,71,1) |SdlTCPConnection(5,100,14,707326)
|5,100,14,707326.4^10.36.100.140^^ |*TraceFlagOverrode
53138763.001 |09:05:19.762 |AppInfo |SIPTcp - SdlRead bufferLen=5000
53138763.002 |09:05:19.762 |AppInfo |//SIP/Stack/Error/0x0/httpish_cache_header_val: DROPPING
unregistered header Locus: c904ecb1-d286-11e6-bfdf-b60ed914549d
53138763.003 |09:05:19.762 |AppInfo |//SIP/Stack/Info/0x0/httpish_msg_process_network_msg:
Content Length 4068, Bytes Remaining 3804
53138763.004 |09:05:19.762 |AppInfo |//SIP/Stack/Info/0x0/ccsip_process_network_message:
process_network_msg: not complete
53138763.005 |09:05:19.762 |AppInfo |SIPTcp - Ignoring large message from %Expressway-
C_IP%:[5060]. Only allow up to 5000 bytes. Resetting connection.
```

Une fois la boîte de dialogue SIP épuisée, Cisco Webex enverra un message de refus SIP 603 entrant à l'Expressway-E, comme indiqué dans l'exemple de journal.

Expressway-E Traces

```
2017-01-04T09:05:40.645-05:00 vcs-expressway tvcs: UTCTime="2017-01-04 14:05:40,645"
Module="network.sip" Level="DEBUG": Action="Received" Local-ip="%Exp-E%" Local-port="25150" Src-
ip="%Webex_IP%" Src-port="5062" Msg-Hash="2483073756671246315" SIPMSG: SIP/2.0 603 Decline
```

Comme mentionné précédemment, il existe trois scénarios différents dans lesquels vous pouvez voir ce comportement. Par souci de clarté, les échantillons de journalisation présentés dans cette illustration correspondent à la situation 3, soit celle de l'envoi de l'appel sortant vers Cisco Webex sous forme d'offre retardée. Solution :

1. Connectez-vous à Unified CM.
2. Accédez à System > Service Parameters.
3. Sélectionnez le serveur qui exécute le service Call Manager.

4. Sélectionnez le service Cisco Call Manager lorsque vous y êtes invité.
5. Sélectionnez l'option avancée.
6. Sous les Paramètres de Clusterwide (Device - SIP) modification des paramètres de la SIP Max Entrant Message Taille à 18000.
7. Sélectionnez Enregistrer.
8. Répétez ce processus pour chaque nœud d'Unified CM qui exécute le service de Cisco Call Manager.

Note: Pour qu'un téléphone IP, un terminal de collaboration ou une ligne principale SIP puisse tirer parti de cette configuration, il faut un redémarrage. Ces périphériques peuvent être redémarrés individuellement pour minimiser l'impact sur l'environnement. NE PAS réinitialiser tous les périphériques du CUCM sauf si vous savez qu'il est absolument acceptable de le

faire. **Annexe Outils de dépannage Expressway** Fonction de vérification de schéma L'Expressway dispose d'un utilitaire de vérification des motifs qui est utile lorsque vous voulez tester si un modèle correspond à un alias particulier et est transformé de manière attendue. La fonction se trouve sur l'Expressway sous l'option de menu Maintenance > Tools > Check pattern. La plupart du temps, ceci est utilisé si vous voulez tester si votre regex de règle de recherche va correctement faire correspondre un alias à une chaîne de modèle, puis éventuellement effectuer une manipulation réussie de la chaîne. Pour Hybrid Call Service Connect, vous pouvez également vérifier si FQDN de grappe Unified CM peut faire une correspondance pour la chaîne de caractères de schéma que vous mettez au point pour FQDN de grappe Unified CM. Lorsque vous utilisez cet utilitaire, n'oubliez pas que l'appel sera acheminé selon les paramètres de FQDN de grappe d'Unified CM décrits dans l'en-tête de routage, et pas selon l'URI de destination. Pour exemple, si l'invitation suivante est arrivée dans l'Expressway, vous pouvez mettre à l'essai les fonctionnalités de schéma par rapport à cucm.rtp.ciscotac.net, plutôt que jorobb@rtp.ciscotac.net.

```
SIPMSG:
|INVITE sip:jorobb@rtp.ciscotac.net SIP/2.0
Via: SIP/2.0/TLS 192.168.1.6:7003;egress-
zone=HybridCallServiceTraversal;branch=z9hG4bKcac6d95278590991a2b516cf57e75827371;proxy-call-
id=abcba873-eaae-4d64-83b4-c4541d4e620c;rport
Via: SIP/2.0/TLS 192.168.1.6:5073;branch=z9hG4bK837b03f2cd91b6b19be4fc58edb251bf12;x-cisco-
local-service=nettle;received=192.168.1.6;rport=41913;ingress-zone=DefaultZone
Via: SIP/2.0/TLS 64.102.241.236:5061;egress-
zone=DefaultZone;branch=z9hG4bK524f89592d00ffc45b7b53000271676c370.88b5177ac4d7cfcae1eb8f8be78da
055;proxy-call-id=2db939b2-a49b-4307-8d96-23716a2c090b;received=172.16.2.2;rport=25010
Via: SIP/2.0/TLS
192.168.4.150:5062;branch=z9hG4bK92f9ef952712e6610c3e6b72770c1230;received=148.62.40.63;rport=39
986;ingress-zone=HybridCallServicesDNS
Via: SIP/2.0/TLS 127.0.0.1:5070;branch=z9hG4bK-313634-
3d27a6f914badee6420287903c9c6a45;rport=45939
Call-ID: 3e613afb185751cdf019b056285eb574@127.0.0.1
CSeq: 1 INVITE
Contact: <sip:192.168.1.6:5073;transport=tls>
From: "pstoiano test" <sip:pstoiano-test@dmzlab.call.ciscopark.com>;tag=145765215
To: <sip:jorobb@rtp.ciscotac.net>
Max-Forwards: 15
Route:
```

Afin d'utiliser le modèle de vérification pour tester le routage de règle de recherche d'en-tête de route Hybrid Call Service Connect, procédez comme suit :

1. Accédez à Maintenance > Outils > Modèle de vérification.
2. Pour l'alias, saisissez le nom de domaine complet du cluster Unified CM.

3. Définissez le type de modèle sur Préfixe.
4. Définissez la chaîne de motifs sur Unified CM Cluster FQDN.
5. Définissez le comportement du modèle sur Leave.
6. Sélectionnez Vérifier le modèle.

Si les règles de recherche sur l'Expressway sont configurées correctement, il est fort probable que s'ensuive un message confirmant la réussite. Voici un exemple de test de modèle de vérification réussi, comme l'illustre l'image.

Check pattern

Alias:

Pattern type:

Pattern string:

Pattern behavior:

Result







Result	Succeeded
Details	Alias matched pattern
Alias	cucm.rtp.ciscotac.net

La raison pour laquelle cela a réussi est que cet alias (cucm.rtp.ciscotac.net) correspond à la chaîne de modèle de préfixe de (cucm.rtp.ciscotac.net). Afin de comprendre comment un appel est acheminé en fonction de ces résultats, vous pouvez utiliser l'utilitaire de localisation Expressway décrit. Fonction de localisation La fonction de localisation de l'Expressway est utile si vous souhaitez vérifier si l'Expressway peut acheminer un appel vers une zone précise selon un alias donné. C'est possible sans passer un appel réel. La fonction se trouve sur l'Expressway sous l'option de menu Maintenance > Outils > Localiser. Vous verrez des instructions sur la façon d'utiliser la fonctionnalité Localiser sur l'Expressway-C pour déterminer si le serveur peut acheminer un appel en fonction du nom de domaine complet du cluster Unified CM trouvé dans l'en-tête de route SIP.

1. Accédez à Maintenance > Outils > Rechercher.
2. Entrez le nom de domaine complet du cluster Unified CM dans le champ Alias.
3. Sélectionnez SIP comme protocole.
4. Sélectionnez votre zone de client Cisco Webex Hybrid Traversal pour la source.
5. Sélectionnez Localiser.

En bas de l'interface, vous voyez désormais les résultats de recherche. Voici un exemple du test d'exemple qui a été exécuté avec les résultats correspondants, comme illustré dans l'image.

Locate

Locate	
Alias	* cucm.rtp.ciscotac.net 
Hop count	* 5 
Protocol	SIP 
Source	Hybrid Call Service Traversal 
Authenticated	Yes 
Source alias	<input type="text"/> 

Locate

Voici les résultats de Locate. Les valeurs d'intérêt sont codées. Ces résultats montrent :

- L'alias pourrait être acheminé (Vrai)
- Des renseignements sur la source (nom ou type de zone)
- Des renseignements sur la destination (alias acheminé)
- La règle de recherche en correspondance (routage intrant de Hybrid Call Service)
- Zone vers laquelle l'appel sera envoyé (CUCM11)

```
Search (1)
State: Completed
Found: True
Type: SIP (OPTIONS)
SIPVariant: Standards-based
CallRouted: True
CallSerial Number: ae73fb64-c305-457a-b7b3-59ea9688c630
Tag: 473a5b19-9a37-40bf-bbee-6f7bc94e7c77
Source (1)
Authenticated: True
Aliases (1)
Alias (1)
Type: Url
Origin: Unknown
Value: xcom-locate
Zone (1)
Name: Hybrid Call Service Traversal
Type: TraversalClient
Path (1)
Hop (1)
Address: 127.0.0.1
Destination (1)
Alias (1)
Type: Url
Origin: Unknown
Value: sip:cucm.rtp.ciscotac.net
StartTime: 2017-09-24 09:51:18
Duration: 0.01
SubSearch (1)
Type: Transforms
Action: Not Transformed
ResultAlias (1)
Type: Url
Origin: Unknown
Value: cucm.rtp.ciscotac.net
SubSearch (1)
Type: Admin Policy
Action: Proxy
ResultAlias (1)
Type: Url
Origin: Unknown
```


Value: cucm.rtp.ciscotac.net
SubSearch (1)
Type: FindMe
Action: Proxy
ResultAlias (1)
Type: Url
Origin: Unknown
Value: cucm.rtp.ciscotac.net
SubSearch (1)
Type: Search Rules
SearchRule (1)
Name: as is local
Zone (1)
Name: LocalZone
Type: Local
Protocol: SIP
Found: False
Reason: Not Found
StartTime: 2017-09-24 09:51:18
Duration: 0
Gatekeeper (1)
Address: 192.168.1.5:0
Alias (1)
Type: Url
Origin: Unknown
Value: cucm.rtp.ciscotac.net
Zone (2)
Name: LocalZone
Type: Local
Protocol: H323
Found: False
Reason: Not Found
StartTime: 2017-09-24 09:51:18
Duration: 0
Gatekeeper (1)
Address: 192.168.1.5:0
Alias (1)
Type: Url
Origin: Unknown
Value: cucm.rtp.ciscotac.net
SearchRule (2)
Name: Hybrid Call Service Inbound Routing
Zone (1)
Name: CUCM11
Type: Neighbor
Protocol: SIP
Found: True
StartTime: 2017-09-24 09:51:18
Duration: 0
Gatekeeper (1)
Address: 192.168.1.21:5065
Alias (1)
Type: Url
Origin: Unknown
Value: cucm.rtp.ciscotac.net

Journaux de diagnostic Quand vous cherchez à régler un problème d'appel ou de support pour un appel qui traverse la solution Expressway, vous devez utiliser la journalisation de diagnostic. Cette fonctionnalité d'Expressway donne au spécialiste en ingénierie des renseignements très détaillés au sujet de toutes les décisions logiques prises sur l'Expressway au fil de la transmission des appels. Vous pouvez consulter les messages SIP au complet, la manière dont l'Expressway transmet un appel et la manière dont l'Expressway configure les canaux de support. La journalisation de diagnostic comprend un certain nombre de différents modules qui s'y intègrent.

Les niveaux de journalisation peuvent être mis au point afin de présenter les éléments suivants : FATAL, ERROR, WARN, INFO, DEBUG, TRACE. Par défaut, tout est réglé sur INFO qui capture presque tout ce dont vous avez besoin pour diagnostiquer un problème. De temps en temps, vous devrez peut-être rajuster le niveau de journalisation d'un module en particulier, pour qu'il passe au niveau DEBUG, afin de mieux comprendre ce qui se passe. Les étapes ci-dessous illustrent comment vous pouvez régler les niveaux de journalisation du module `developer.ssl` qui est chargé de fournir les renseignements sur les prises de contact mutuelles de TLS.

1. Connectez-vous au serveur Expressway (à effectuer sur l'Expressway-E et C).
2. Accédez à Maintenance > Diagnostics > Advanced > Support Log configuration.
3. Faites défiler jusqu'au module de la mise au point, dans ce cas-ci, `developer.ssl` et cliquez dessus.
4. En regard du paramètre Level, choisissez DEBUG dans le menu.
5. Cliquez sur Save.

À ce moment-ci, vous êtes prêt à saisir l'information de la journalisation de diagnostic :

1. Connectez-vous au serveur Expressway (à effectuer sur l'Expressway-E et C).
2. Accédez à Maintenance > Diagnostics > Diagnostic logging.
3. Cliquez sur Démarrer un nouveau journal (vérifiez que vous cochez l'option `tcpdump`).
4. Reproduisez le problème.
5. Cliquez sur Arrêter la journalisation.
6. Cliquez sur Télécharger le journal.

Pour la journalisation de diagnostic d'Expressway, n'oubliez pas que vous voudrez débiter la journalisation de l'Expressway-C et de l'Expressway-E en parallèle : tout d'abord, démarrez la journalisation sur l'Expressway-E, puis allez sur l'Expressway-C et démarrez-la. À ce stade-là, vous pourrez ensuite reproduire le problème. Note: Actuellement, l'ensemble du journal de diagnostic Expressway/VCS ne contient pas d'informations sur le certificat du serveur Expressway ou la liste des autorités de certification de confiance. Dans un cas où cette fonctionnalité vous

serait utile, veuillez joindre votre dossier à [ce défaut](#).

Informations connexes

- [Guide de déploiement de Cisco Webex Hybrid Call Services](#)
- [Guide de conception Cisco Webex Hybrid](#)
- [Guide de l'administrateur Cisco Expressway](#)
- [Support et documentation techniques - Cisco Systems](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.